Policy Management

Benutzerhandbuch

Version R9

Deutsch

März 19, 2015

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

©2015 Kaseya. All rights reserved. | www.kaseya.com

Inhalt

Policy Management Überblick 1
Policy Management Modulvoraussetzungen 3
Dashboard 3
Protokolle 4
Richtlinienmatrix 4
Richtlinien 6
Richtlinien – Ordnerstruktur 7
Richtlinien – Registerkarte "Einstellungen" 8
Richtlinien – Registerkarte "Einstellungen" – Agent-Menü 9
Richtlinien – Registerkarte "Einstellungen" – Agent-Prozedur 10
Richtlinien – Registerkarte "Einstellungen" – Benachrichtigungen 10
Richtlinien – Registerkarte "Einstellungen" – Auditplan 12
Richtlinien – Registerkarte "Einstellungen" – Anmeldung 12
Richtlinien – Registerkarte "Einstellungen" – Anmeldedaten 14
Richtlinien – Registerkarte "Einstellungen" – Datei verteilen 15
Richtlinien – Registerkarte "Einstellungen" – Ereignisprotokolleinstellungen 15
Richtlinien – Registerkarte "Einstellungen" – Kaseya AntiMalware 16
Richtlinien – Registerkarte "Einstellungen" – Kaseya Antivirus 16
Richtlinien – Registerkarte "Einstellungen" – Kaseya Security 16
Richtlinien – Registerkarte "Einstellungen" – LAN-Cache 17
Richtlinien – Registerkarte "Einstellungen" – Protokollhistorie 17
Richtlinien – Registerkarte "Einstellungen" – Rechnerprofil 18
Richtlinien – Registerkarte "Einstellungen" – Monitor-Sets 18
Richtlinien – Registerkarte "Einstellungen" – Patchdateiquelle 19
Richtlinien – Registerkarte "Einstellungen" – Patch-Verfahren-Planung 20
Richtlinien – Registerkarte "Einstellungen" – Patch-Neustart-Aktion 21
Richtlinien – Registerkarte "Einstellungen" – Patch-Einstellungen 23
Richtlinien – Registerkarte "Einstellungen" – Automatische Windows-Aktualisierung patchen 24
Richtlinien – Registerkarte "Einstellungen" – Schutz 24
Richtlinien – Registerkarte "Einstellungen" – Remote Control 25
Richtlinien – Registerkarte "Einstellungen – Zuweisung Softwarebereitstellungsprofil 26
Richtlinien – Registerkarte "Einstellungen" – Neustart für Softwarebereitstellung 26
Richtlinien – Registerkarte "Einstellungen" – Zuweisung Softwarebereitstellungsscan 28
Richtlinien – Registerkarte "Einstellungen" – Alarme unterbrechen 28
Richtlinien – Registerkarte "Einstellungen" – Liste nach Scan aktualisieren 29
Richtlinien – Registerkarte "Einstellungen" – Arbeitsverzeichnis 30
Einstellungen 30
Organisationen/Rechnergruppen 31

Rechner **33**
Policy Management – Agent-Richtlinienstatus **34**
Policy Management – Richtliniendaten & Zuordnung **35**
Glossar **37**
Inhaltsverzeichnis **43**

Policy Management Überblick

Das **Policy Management** (KPM)-Modul verwaltet *Agent-Einstellungen nach Richtlinie*.

- Sobald Richtlinien Rechnern, Rechnergruppen oder Unternehmen zugewiesen sind, *werden Richtlinien automatisch verteilt*, ohne dass der Benutzer weiter eingreifen muss.
- Jede Richtlinie umfasst Unterkategorien von Agent-Einstellungen, die sogenannten *Richtlinienobjekte*.
- Richtlinien können nach Rechner-ID, Rechnergruppe oder Unternehmen zugewiesen werden. Es muss eine Ansichtsdefinition verwendet werden, um die von der Richtlinie betroffenen Rechner zu filtern.
- Wird die Verknüpfung eines Rechners mit einer Rechnergruppe, einem Unternehmen oder einer Ansicht geändert, so werden die entsprechenden Richtlinien automatisch neu implementiert.
- Jedem Rechner können mehrere Richtlinien zugewiesen werden. Wenn sich Richtlinien widersprechen, bestimmen Regeln zur Richtlinienzuweisung, welche Richtlinien befolgt und welche ignoriert werden.
- Ein Konformitätszyklus überprüft, dass jeder Rechner die angewendeten Richtlinien erfüllt. VSABenutzer können den Status jedes Rechners überprüfen, um sicherzustellen, dass er die angewendeten Richtlinien erfüllt.
- Eine Richtlinie kann überschrieben werden. Die Bedingung einer **Policy Management**-Richtlinienüberschreibung besteht, wenn Agent-Einstellungen für einen Rechner manuell eingestellt wurden, außerhalb des **Policy Management**-Moduls. Werden zum Beispiel Änderungen am Agent-Menü eines Rechners über die Seite **Agent-Menü** im **Agent**-Modul vorgenommen, so wird eine Überschreibbedingung für diesen Agent-Rechner erstellt. **Policy Management**Richtlinien werden von da an ignoriert. Richtlinienüberschreibungen können auch gelöscht werden.
- Richtlinien können mit System > **Import-Center** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#6963.htm)* importiert und exportiert werden.
- Ein **System-Cabinet** *(siehe 40)* bietet integrierte Richtlinien, die Best-Practice-Lösungen für gewöhnliche IT-Verwaltungsaufgaben darstellen. Richtlinien können mithilfe des **Systems Management Configuration Installationsassistenten** *(http://help.kaseya.com/webhelp/DE/SSP/9000000/index.asp#11220.htm)* und dieser System-Cabinet-Richtlinien automatisch für ein Unternehmen konfiguriert werden.

Zusätzliche Konditionen

- *Anwenden einer Richtlinie* bedeutet, dass die Änderungen, die an ihren Richtlinienobjekten vorgenommen wurden, *zur Verteilung gekennzeichnet* werden. Bereitstellung bedeutet, dass die angewendeten Änderungen auf den Zielrechnern mithilfe der Seite **Einstellungen** *(siehe 30)* verteilt werden, basierend auf dem Bereitstellungsintervallsatz. Da die Bereitstellung einige Zeit in Anspruch nehmen kann, *erfüllt der Zielrechner möglicherweise nicht die Richtlinie* hinsichtlich der Dauer zwischen der Richtlinienanwendung und der Richtlinienbereitstellung.
- *Ausstehende Änderungen* sind Änderungen an Richtlinien oder Richtlinienobjekten, die zwar gespeichert, aber noch nicht angewendet wurden.

Konfiguration

1. Konfigurieren Sie allgemeine Einstellungen für das gesamte **Policy Management**-Modul über die Seite **Einstellungen** *(siehe 30)*.
2. Definieren Sie Richtlinien für die Agent-Einstellung über die Seite **Richtlinien** *(siehe 6)*.
3. Wenden Sie Richtlinien an auf:
   - Unternehmen und Rechnergruppen mithilfe der Seite **Unternehmen / Rechnergruppen** *(siehe 31)*

- einzelne Rechner mithilfe der Seite **Rechner** *(siehe 33)*. Sie können auch **Policy Management**-Richtlinienüberschreibungen über diese Seite löschen, sodass die angewendeten Richtlinien in Kraft treten können.

  Hinweis: Richtlinien werden verteilt, nachdem sie angewendet werden.

4. Überwachen Sie die Einhaltung der Richtlinien über die Seiten **Richtlinienmatrix** *(siehe 4)* und **Dashboard** *(siehe 3)*.
5. Überwachen Sie die **Policy Management**-Aktivität über die Seite **Protokolle** *(siehe 4)*.

Erstellen von Richtlinien basierend auf Agent-Vorlagen

Sie können Agent-Einstellungen, die von einer Agent-Vorlage verwaltet werden, nach **Policy Management** migrieren. Die Schaltfläche **Von Vorlage importieren** auf der Seite **Richtlinien** *(siehe 6)* erstellt eine Richtlinie auf Grundlage der Agent-Einstellungen, die von der Seite Agent > **Kopiereinstellungen** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#547.htm)* unterstützt werden.

Hinweis: Siehe KPMSystemanforderungen.

Funktionen	Beschreibung
Überblick	Stellt den Policy Management-Workflow grafisch dar.
Dashboard *(siehe 3)*	Bietet eine Dashboard-Ansicht der Policy Management-Aktivitäten.
Protokolle *(siehe 4)*	Zeigt ein Protokoll der Policy Management-Modulaktivität an.
Richtlinienmatrix *(siehe 4)*	Zeigt den Richtlinienstatus aller Rechner an, die innerhalb Ihres Scope liegen. Ein Richtlinienstatussymbol wird für alle Rechner in der Spalte ganz links auf dieser Seite angezeigt.
Richtlinien *(siehe 6)*	Definiert Agent-Einstellungen nach Richtlinie, einschließlich • Agent-Menü • Benachrichtigungen • Auditplan • Anmeldung • Anmeldedaten • Dateien verteilen – Dieses Richtlinienobjekt ist nicht einem **SaaS** *(siehe 40)*-basiertem VSA verfügbar. • Ereignisprotokolleinstellungen • Kaseya Anti-Malware • Kaseya AntiVirus • Kaseya Security • Protokollhistorie • Rechnerprofil • Monitor-Sets • Patchdateiquelle • Patch-Verfahren-Planung • Patch-Neustart-Aktion • Patch-Einstellungen • Automatische Windows-Aktualisierung patchen • Schutz • Remote Control • Arbeitsverzeichnis
Einstellungen *(siehe 30)*	Plant das Intervall für die automatische Bereitstellung aller

	Richtlinien auf allen zugewiesenen Rechnern.
Organisationen/Rechnergruppen *(siehe 31)*	Weist Richtlinien Unternehmen und Rechnergruppen zu.
Rechner *(siehe 33)*	Weist Richtlinien einzelnen Rechnern zu.

Policy Management Modulvoraussetzungen

Kaseya Server

- Das Policy Management R9-Modul erfordert VSA R9.

Hinweis: Siehe allgemeine **Systemanforderungen** *(http://help.kaseya.com/WebHelp/EN/VSA/9000000/reqs/index.asp#home.htm).*

Dashboard

Policy Management > Dashboard

Die Seite **Dashboard** bietet eine Dashboard-Ansicht der **Policy Management**-Aktivitäten, darunter:

- **Agentstatus** – Zeigt ein Tortendiagramm des Richtlinien-Konformitätsstatus nach Agent-Anzahl und Agent-Prozentzahl an. Klicken Sie auf ein Kreissegment, um ein **Agentstatus-Detail-Raster** des Richtlinien-Konformitätsstatus der Rechner der Mitglieder anzuzeigen. Innerhalb dieses Fensters können Sie auf die Schaltfläche **Gehe zum Bildschirm Rechner Richtlinien-Verwaltung** klicken, um die Seite **Rechner** *(siehe 33)* anzuzeigen und Richtlinien-Zuordnungen der einzelnen Rechner zu aktualisieren.

  – `Richtlinien erfüllende Agents` – Die Agent-Einstellungen für diesen Rechner entsprechen den Einstellungen aller diesem Rechner zugeordneten Richtlinien.

  – `Zur Bereitstellung gekennzeichnete Agents`– Es wurde mindestens eine diesem Rechner zugewiesene Richtlinie geändert und deren Bereitstellung geplant.

  – `Agents ohne Richtlinie` – Diesem Rechner sind keine *angewendeten* Richtlinien zugewiesen.

  – `Agents, die Richtlinien nicht mehr erfüllen` – Mindestens eine Agent-Einstellung entspricht mindestens einer aktiven Richtlinie, die diesem Rechner zugewiesen ist, nicht.

  – `Überschriebene Agents` – Mindestens eine Agent-Einstellung entspricht mindestens einer aktiven Richtlinie, die diesem Rechner zugewiesen ist, *aufgrund einer Benutzerüberschreibung* nicht. Eine Überschreibung tritt auf, wenn eine Agent-Einstellung manuell von einem VSA-Benutzer an einem beliebigen Ort im System vorgenommen wird. Wenn auch nur eine einzelne Agent-Einstellung in einer einem Rechner zugewiesenen Richtlinie überschrieben wird, werden keine weiteren Agent-Einstellungen in dieser Richtlinie auf diesem Rechner durchgesetzt. Andere demselben Rechner zugewiesenen Richtlinien behalten ihre Gültigkeit.

- **Richtlinienstatus** – Zeigt ein Tortendiagramm des Richtlinienstatus nach Richtlinienstatus-Anzahl und Richtlinienstatus-Prozentzahl an.
  - `Bereitgestellte Richtlinien` – Richtlinien, die an mindestens einen Agent bereitgestellt wurden.
  - `Nicht zugeordnete Richtlinien` – Richtlinien, die keinem Agent zugewiesen sind.

- `Richtlinien mit nicht angewendeten Änderungen` – Bereitgestellte Richtlinien mit gespeicherten Änderungen, die noch nicht angewendet wurden. Diese Richtlinien werden durch ein -Symbol auf der Seite **Richtlinien** *(siehe 6)* angezeigt.

- **Noch offene Ereignisse** – Listet Richtlinienänderungen auf oder überschreibt manuell diejenigen, die noch nicht verarbeitet wurden. Noch offene Ereignisse werden in regelmäßigen Intervallen verarbeitet, weshalb dieses Raster nicht viele Daten enthält.

Protokolle

Policy Management > Protokolle

Die Seite **Protokolle** zeigt ein Protokoll der **Policy Management**-Modulaktivität mit Folgendem an:

- **Ereignis-ID**
- **Ereignisname**
- **Meldung**
- **Admin**
- **Ereignis-Datum**

Diese Tabelle unterstützt **auswählbare Spalten, Spaltensortierung, Spaltenfilter und flexible Spaltenbreite** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#6875.htm)*.

Richtlinienmatrix

Policy Management > Richtlinienmatrix

Die Seite **Richtlinienmatrix** zeigt den Richtlinienstatus aller Rechner an, die innerhalb Ihres Scope liegen. Ein Richtlinienstatussymbol wird für alle Rechner in der Spalte ganz links auf dieser Seite angezeigt.

Richtliniendetails

Durch Fahren mit dem Cursor über ein Richtlinienstatussymbol auf dieser Seite wird das Fenster **Richtliniendetails** angezeigt. Das Fenster **Richtliniendetails** hat zwei Registerkarten.

- **Details Richtlinienobjektstatus** – Führt alle Richtlinien und *angewendeten Richtlinienkategorien* bei einem ausgewählten Rechner auf.
- **Gültige Rechner-Richtlinieneinstellung** – Führt alle *gültigen Richtlinieneinstellungen* bei einem ausgewählten Rechner auf. Da mehr als eine Richtlinie auf einen Rechner angewendet werden kann, können manche angewendeten Einstellungen auf Grundlage der **Regeln zur Richtlinienzuweisung** *(siehe 31)* ignoriert werden.

Tabellenspalten

- **(Richtlinienstatussymbol)**

  - `In Compliance` – Die Agent-Einstellungen für diesen Rechner entsprechen den Einstellungen aller diesem Rechner zugewiesenen Richtlinien. Keine Benutzeraktion ist erforderlich.

  - `Marked for Deployment` – Es wurde mindestens eine diesem Rechner zugewiesene Richtlinie geändert und so geplant, dass sie bereitgestellt wird. Keine Benutzeraktion ist erforderlich.

  - `No Policy Attached` – Diesem Rechner sind keine *angewendeten* Richtlinien zugewiesen. Erwägen Sie, diesem Rechner *angewendete* Richtlinien zuzuweisen.

  - `Out of Compliance` – Mindestens eine Agent-Einstellung entspricht nicht mindestens

einer aktiven Richtlinie, die diesem Rechner zugewiesen ist. Ermitteln Sie mithilfe des Fensters **Richtliniendetails** die bestimmten Richtlinien und Einstellungen, die diese Nichtübereinstimmung verursachen.

- `Overridden` – Mindestens eine Agent-Einstellung entspricht nicht mindestens einer aktiven Richtlinie, die diesem Rechner zugewiesen ist, *aufgrund einer Benutzerüberschreibung*. Eine Überschreibung tritt auf, wenn eine Agent-Einstellung manuell von einem VSA-Benutzer an einem beliebigen Ort im System vorgenommen wird. Bestätigen Sie mithilfe des Fensters **Richtliniendetails**, dass das Überschreiben bestimmter Richtlinien und Einstellungen richtig ist. Wenn auch nur eine einzelne Agent-Einstellung in einer einem Rechner zugewiesenen Richtlinie überschrieben wird, werden keine weiteren Agent-Einstellungen in dieser Richtlinie auf diesem Rechner durchgesetzt. Andere demselben Rechner zugewiesenen Richtlinien behalten ihre Gültigkeit.

- `Inactive` – *Dieser Richtlinienstatus wird nur im Fenster* **Richtliniendetails** *angezeigt.* Wenn einem Rechner mehrere Richtlinien zugewiesen werden und sich die Agent-Einstellungen widersprechen, so wird durch **Regeln zur Richtlinienzuweisung** *(siehe 31)* festgelegt, welche Agent-Einstellungen befolgt und welche ignoriert werden. Ignorierte Einstellungen werden als inaktiv angezeigt. Als Rechnerstatus kann das Richtlinienstatussymbol `In Compliance` angezeigt werden, während im Fenster *Richtliniendetails* bestimmte Agent-Einstellungen in bestimmten Richtlinien als `Inactive` angezeigt werden. Dieses Verhalten wird erwartet. Keine Benutzeraktion ist erforderlich.

- **Rechner-ID** – Die Rechner-ID, der eine Richtlinie zugewiesen ist. Für eine Rechner-ID werden mehrere angezeigt, eine Zeile pro Richtlinie, die dieser Rechner-ID zugewiesen ist.
- **Rechnergruppe** – Die Rechnergruppe, von der diese Rechner-ID Mitglied ist.
- **Richtlinie** – Die diesem Rechner zugewiesene Richtlinie.
- **Richtlinien-Objekttypen** – Die Kategorien der Agent-Einstellungen, die mit dieser Richtlinie zugewiesen wurden. Eine Richtlinienart in rotem Text zeigt an, dass diese Richtlinienart durch eine andere Richtlinie überschrieben wurde und nicht gilt.
- **Verknüpft durch** – Der Objekttyp, der zur Verknüpfung des Rechners mit einer Richtlinie verwendet wurde: Rechner, Rechnergruppe oder Unternehmen.
- **Ansicht** – Mit einer Richtlinie verknüpfte Ansichten. Eine Ansicht *filtert* die mit einer Richtlinie verknüpften Rechner.
- **Aktiv** – Wenn `Yes`, ist die Richtlinie aktiv. Richtlinien können aktiv oder inaktiv sein, je nach Reihenfolge oder Vorrang, ob sie überschrieben wurden oder nicht erfüllt werden.

Abkürzungen für Richtlinienmatrix

Die folgenden Abkürzungen werden in der Spalte **Richtlinien-Objekttypen** der Seite **Richtlinienmatrix** angezeigt.

Abkürzung	Richtlinien-Objekttyp
AL	Benachrichtigungen
AM	Agent-Menü
AP	Skripting
AS	Auditplan
CD	Anmeldedaten
CI	Anmeldung
DF	Dateien verteilen
EL	Ereignisprotokolleinstellungen
KAM	Kaseya Anti-Malware
KAV	Kaseya Anti-Virus
KES	Kaseya Security

LG	Protokollhistorie
MP	Rechnerprofil
MS	Monitor-Sets
PFS	Patchdateiquelle
PPS	Patch-Verfahren-Planung
PRA	Patch-Neustart-Aktion
PS	Patch-Einstellungen
PT	Schutz
RC	Remote Control
SDP	Zuweisung Softwarebereitstellungsprofil
SDR	Neustart für Softwarebereitstellung
SDS	Scan-Zeitplan für Softwarebereitstellung
WD	Arbeitsverzeichnis
WU	Automatische Windows-Aktualisierung patchen

Richtlinien

Policy Management > Richtlinien

Die Seite **Richtlinien** definiert Agent-Richtlinien. Richtlinien sind in einer **Ordnerstruktur** *(siehe 7)* organisiert. Ein **System-Cabinet** *(siehe 40)* bietet integrierte Richtlinien, die Best-Practice-Lösungen für gewöhnliche IT-Verwaltungsaufgaben darstellen. Richtlinien können mithilfe des **Systems Management Configuration Installationsassistenten** *(http://help.kaseya.com/webhelp/DE/SSP/9000000/index.asp#11220.htm)* und dieser System-Cabinet-Richtlinien automatisch für ein Unternehmen konfiguriert werden.

Registerkarten

- **Einstellungen** *(siehe 8)* – Agent-Richtlinieneinstellungen sind in dieser Registerkarte nach Einstellungskategorie gruppiert. Klicken Sie auf ein Kontrollkästchen für eine Einstellungskategorie, um die Einstellungen für diese Kategorie anzugeben.
- **Rechnergruppen werden zugeordnet** – Die Unternehmen und Rechnergruppen, die einer Richtlinie zugewiesen sind, werden auf dieser Registerkarte angezeigt. Eine Richtlinie wird durch Unternehmen oder Rechnergruppe mithilfe der Seite **Unternehmen / Rechnergruppen** *(siehe 31)* zugewiesen.
- **Zugeordnete Rechner** – *Bestimmen Sie mit dieser Registerkarte die Rechner, die Mitglieder einer Richtlinie sind.* Die Liste der Rechner, die auf dieser Registerkarte angezeigt werden, hängt von folgenden Punkten ab:
  - Den Unternehmen oder Rechnergruppen, die dieser Richtlinie über die Seite **Unternehmen / Rechnergruppen** *(siehe 31)* zugewiesen sind.
  - Den einzelne Rechnern, die dieser Richtlinie über die Seite **Rechner** *(siehe 33)* zugewiesen sind.
  - Der Ansicht, mit der diese Richtlinie über die Registerkarte **Einstellungen** *(siehe 8)* auf der Seite **Richtlinien** verknüpft ist. Eine mit einer Richtlinie verknüpfte Ansicht filtert die Rechnermitgliedschaft in dieser Richtlinie.

    Hinweis: Die mit einer Richtlinie verknüpfte Ansicht wird ignoriert, wenn die Richtlinie *nach Rechner* über die Seite **Rechner** zugewiesen wird.

> **Hinweis:** Ansichten, die von einem anderen Benutzer erstellt wurden und nicht für Sie freigegeben sind, sind nicht für Sie zur Auswahl in der Drop-down-Liste **Ansicht** verfügbar. Wenn ein anderer Benutzer eine Richtlinie mit Ihnen geteilt hat, die zugehörige Ansicht jedoch nicht für Sie freigegeben hat, ist die Richtlinie schreibgeschützt.

- Der aktuell ausgewählten Ansicht im **Rechner-ID/Gruppen-ID-Filter** oben auf der Seite. *Die aktuell ausgewählte Ansicht beschränkt nur die Anzeige von Rechnern in dieser Registerkarte, nicht ob die Rechner Mitglieder dieser Richtlinie sind.*

Erstellen von Agent-Richtlinien

1. Wählen Sie im mittleren Fensterbereich einen Ordner aus.
2. Klicken Sie auf die Schaltfläche **Richtlinie hinzufügen**.
3. Geben Sie einen Namen ein und klicken Sie **OK**.

> **Hinweis:** Der Name der Richtlinie ist auf 100 Zeichen begrenzt. Das Erstellen eines Namens, der über 100 Zeichen enthält, kann dazu führen, dass die Richtlinie abläuft und nicht mehr bearbeitet werden kann.

4. Definieren Sie Agent-Einstellungen in der Registerkarte **Einstellungen** im rechten Fensterbereich.
5. Klicken Sie auf **Speichern**, um die Änderungen an der Richtlinie zu speichern. Eine Richtlinie zeigt ein gelbes Symbol zum Blättern an, wenn sie nur gespeichert, aber noch nicht angewendet wurde.
6. Klicken Sie auf **Speichern und Anwenden**, um die Einstellungen für eine ausgewählte Richtlinie zu speichern und anzuwenden. Anwenden bedeutet, dass die Einstellungen auf zugewiesene Rechner verteilt werden. Durch eine Bestätigungsmeldung können Sie zwischen **Jetzt anwenden** und **Scheduler die Anwendung gestatten** wählen, wodurch die Änderungen mithilfe des Bereitstellungsintervall angewendet werden, welches auf der Seite **Einstellungen** *(siehe 30)* angegeben ist.

Richtlinien – Ordnerstruktur

Policy Management > Richtlinien > Ordnerstruktur

Richtlinien sind in einer Ordnerstruktur im mittleren Fensterbereich organisiert. Verwenden Sie die folgenden Optionen, um Objekte in dieser Ordnerstruktur zu verwalten.

Immer verfügbar

- **(Filter anwenden)** – Geben Sie Text in das Bearbeitungsfeld des Filters ein und klicken Sie dann auf das Trichtersymbol, um das Filtern auf die Ordnerstruktur anzuwenden. Beim Filtern wird nicht zwischen Groß-/Kleinschreibung unterschieden. Eine Übereinstimmung trifft ein, wenn Filtertext irgendwo in der Ordnerstruktur gefunden wird.

Bei Auswahl des Gehäuses

- **Alle ausblenden** – Blendet alle Verzweigungen der Ordnerstruktur aus.
- **Alle ausweiten** – Erweitert alle Verzweigungen der Ordnerstruktur.

Bei Auswahl des Gehäuses oder eines Ordners

- **Ordner hinzufügen** – Erstellt einen neuen Ordner unterhalb des ausgewählten Cabinet oder Ordners.

Bei Auswahl eines Ordners

- **Richtlinie hinzufügen** – Erstellt eine neue Richtlinie in dem ausgewählten Ordner der Ordnerstruktur.
- **Richtlinien anwenden** – Wendet alle Änderungen auf alle Richtlinien in einem ausgewählten Ordner an.
- **Von Vorlage importieren** – Erstellt eine Richtlinie auf Grundlage der Agent-Einstellungen, die von der Seite Agent > **Kopiereinstellungen** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#547.htm)* unterstützt werden. Verwenden Sie diese Funktion, um Rechnervorlagen auf Richtlinien zu migrieren.
- **Umbenennen** – Benennt einen ausgewählten Ordner um.
- **Löschen** – Löscht einen ausgewählten Ordner.
- **Gemeinsam nutzen** – **Gibt** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#5537.htm)* einen Richtlinienordner frei.

Bei Auswahl einer Richtlinie

- **Speichern unter** – Speichert eine Richtlinie unter einem neuen Namen.
- **Löschen** – Löscht eine ausgewählte Richtlinie.
- **Richtlinie anwenden** – Wendet Richtlinienänderungen auf eine ausgewählte Richtlinie an.

Richtlinien – Registerkarte "Einstellungen"

Policy Management > Richtlinien > Registerkarte ''Einstellungen''

Agent-Richtlinieneinstellungen sind in dieser Registerkarte nach Kategorie gruppiert. Klicken Sie auf ein Kontrollkästchen für eine Kategorie, um die Einstellungen für diese Kategorie anzugeben.

Aktionen

- **Speichern** – Speichert die Einstellungen für eine ausgewählte Richtlinie, ohne diese Einstellungen auf zugeordnete Rechner zu verteilen. Eine Richtlinie zeigt ein gelbes Symbol zum Blättern an, wenn sie nur gespeichert, aber noch nicht angewendet wurde.
- **Speichern und Anwenden** – Speichert die Einstellungen für eine ausgewählte Richtlinie und wendet sie an. Anwenden bedeutet, dass die Einstellungen auf zugewiesene Rechner verteilt werden. Durch eine Bestätigungsmeldung können Sie zwischen **Jetzt anwenden** und **Scheduler die Anwendung gestatten** wählen, wodurch die Änderungen mithilfe des Bereitstellungsintervall angewendet werden, welches auf der Seite **Einstellungen** *(siehe 30)* angegeben ist.
- **Abbrechen** – Bricht Änderungen an Einstellungen ab, ohne sie zu speichern bzw. zu übernehmen.

Überschrift

- **Name** – Der Name einer Richtlinie.
- **Beschreibung** – Die Beschreibung einer Richtlinie.
- **Ansicht** – Eine Ansichtsdefinition, die mit der Richtlinie verknüpft ist. Wenn eine Richtlinie einer Ansichtsdefinition zugewiesen wurde, so gilt die Richtlinie nur noch für Rechner, die Mitglieder dieser Ansicht sind.
  - Auf der Seite Richtlinien *muss* einer Richtlinie eine Ansicht zugewiesen werden, um eine Richtlinie mit der Seite **Unternehmen/Rechnergruppen** *(siehe 30)* zuzuweisen. *So wird verhindert, dass eine Richtlinie unbeabsichtigt allen Rechner in VSA zugewiesen wird.* Eine Richtlinie ohne angegebene Ansicht wird mit einem roten Symbol zum Blättern in der Richtlinienstruktur auf der Seite **Unternehmen/Rechnergruppen** angezeigt und gibt so an, dass sie nicht zugewiesen werden kann. Ein Ordner mit einem roten Ausrufezeichen wird in der Richtlinienstruktur angezeigt, wenn diese mindestens eine Richtlinie ohne angegebene Ansicht enthält. Beim Zuweisen eines gesamten Richtlinienordners zu einem Unternehmen oder einer Rechnergruppe werden Richtlinien ohne angegebene Ansicht ignoriert.

- Es ist *nicht erforderlich*, eine Richtlinie einer Ansicht zuzuweisen, wenn die Richtlinie nur mithilfe der Seite **Rechner** *(siehe 33)* zugewiesen wird.
- Ansichten, die von einem anderen Benutzer erstellt wurden und nicht für Sie freigegeben sind, sind nicht für Sie zur Auswahl in der Drop-down-Liste **Ansicht** verfügbar. Wenn ein anderer Benutzer eine Richtlinie mit Ihnen geteilt hat, die zugehörige Ansicht jedoch nicht für Sie freigegeben hat, ist die Richtlinie schreibgeschützt.

Einstellungskategorien

- **Richtlinien – Registerkarte "Einstellungen" – Agent-Menü** *(siehe 9)*
- **Richtlinien – Registerkarte "Einstellungen" – Agent-Verfahren** *(siehe 10)*
- **Richtlinien – Registerkarte "Einstellungen" – Benachrichtigungen** *(siehe 10)*
- **Richtlinien – Registerkarte "Einstellungen" – Auditplan** *(siehe 12)*
- **Richtlinien – Registerkarte "Einstellungen" – Anmeldung** *(siehe 12)*
- Richtlinien – Registerkarte "Einstellungen" – Data Backup
- Richtlinien – Registerkarte "Einstellungen" – Desktop-Richtlinie und -Migration
- **Richtlinien – Registerkarte "Einstellungen" – Anmeldedaten** *(siehe 14)*
- **Richtlinien – Registerkarte "Einstellungen" Datei verteilen** *(siehe 15)* – Dieses Richtlinienobjekt ist nicht in einem **SaaS** *(siehe 40)*-basierten VSA verfügbar.
- **Richtlinien – Registerkarte "Einstellungen" – Ereignisprotokolleinstellungen** *(siehe 15)*
- **Richtlinien – Registerkarte "Einstellungen" – Kaseya AntiMalware** *(siehe 16)*
- **Richtlinien – Registerkarte "Einstellungen" – Kaseya Antivirus** *(siehe 16)*
- **Richtlinien – Registerkarte "Einstellungen" – Kaseya Security** *(siehe 16)*
- **Richtlinien – Registerkarte "Einstellungen" – LAN-Cache** *(siehe 17)*
- **Richtlinien – Registerkarte "Einstellungen" – Protokollhistorie** *(siehe 17)*
- **Richtlinien – Registerkarte "Einstellungen" – Rechnerprofil** *(siehe 18)*
- **Richtlinien – Registerkarte "Einstellungen" – Monitor-Sets** *(siehe 18)*
- **Richtlinien – Registerkarte "Einstellungen" – Patchdateiquelle** *(siehe 19)*
- **Richtlinien – Registerkarte "Einstellungen" – Patch-Verfahren-Planung** *(siehe 20)*
- **Richtlinien – Registerkarte "Einstellungen" – Patch-Neustart-Aktion** *(siehe 21)*
- **Richtlinien – Registerkarte "Einstellungen" – Patch-Einstellungen** *(siehe 23)*
- **Richtlinien – Registerkarte "Einstellungen" – Automatische Windows-Aktualisierung patchen** *(siehe 24)*
- **Richtlinien – Registerkarte "Einstellungen" – Schutz** *(siehe 24)*
- **Richtlinien – Registerkarte "Einstellungen" – Remote Control** *(siehe 25)*
- Richtlinien – Registerkarte "Einstellungen" – Systemsicherung und -wiederherstellung
- Richtlinien – Registerkarte "Einstellungen" – Verwaltung Virtuelle Maschine
- **Richtlinien – Registerkarte "Einstellungen" – Arbeitsverzeichnis** *(siehe 30)*

Richtlinien – Registerkarte "Einstellungen" – Agent-Menü

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Agent-Menü''

Die Kategorie **Agent-Menü** weist einer Richtlinie **Agent-Menü** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#450.htm)*-Einstellungen zu.

- **Agent-Symbol aktivieren** – Aktivieren Sie dieses Kontrollkästchen, um das Agent-Symbol in der Systemablage des verwalteten Rechners anzuzeigen. Deaktivieren Sie dieses Kontrollkästchen,

um das Agent-Symbol auszublenden und die Verwendung von Agent-Menü-Optionen zu verhindern.

- **Über<Agent>** – Aktivieren Sie dies, damit der Rechnerbenutzer auf diese Option klicken kann, um das Feld Info für den installierten Agent anzuzeigen. Die Standard-Optionsbezeichnung `Agent` kann angepasst werden.
- **<Administrator kontaktieren...>** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer auf diese Option klicken kann, um entweder die Seite Portal-Zugang oder eine andere URL anzuzeigen. Die Standard-Optionsbezeichnung `Contact Administrator...` kann angepasst werden.
- **<URL Ihres Unternehmens...>** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer auf diese Option klicken kann, um die im entsprechenden URL-Feld angegebene URL anzuzeigen.
- **Fernsteuerung deaktivieren** – Aktvieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer auf diese Option klicken kann, um die Fernsteuerung auf dem verwalteten Rechner des Benutzers zu *deaktivieren*.
- **Konto festlegen...** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer auf diese Option klicken kann, um seine Rechner-ID.Gruppen-ID.Organisations-ID anzuzeigen und die Kaseya Server-Adresse für die Agent-Anmeldung zu ändern. Die von Ihnen eingegebene, neue IP-Adrresse muss auf einen funktionierenden VSA verweisen. Ansonsten tritt die Änderung der IP-Adresse nicht in Kraft.
- **Aktualisieren** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer eine sofortige vollständige Anmeldung einleiten kann.
- **Beenden** – Aktivieren Sie dieses Kontrollkästchen, damit der Rechnerbenutzer den Agent-Dienst auf dem verwalteten Rechner beenden kann.

Richtlinien – Registerkarte "Einstellungen" – Agent-Prozedur

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Agent-Prozedur''

Die Kategorie **Agent-Verfahren** weist einer Richtlinie **Agent-Prozeduren** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#2845.htm)* zu.

Hinweis: Wenn mehrere Richtlinien demselben Rechner zugewiesen sind, werden alle zugewiesenen Agent-Verfahren in allen zugewiesenen Richtlinien auf diesem Rechner bereitgestellt.

- **Verfahren hinzufügen** – Fügt ein Agent-Verfahren hinzu und plant es.
- **Verfahren entfernen** – Entfernt ein ausgewähltes Agent-Verfahren.

Richtlinien – Registerkarte "Einstellungen" – Benachrichtigungen

Policy Management > Richtlinien > Registerkarte ''Einstellungen > Kontrollkästchen ''Benachrichtigungen''

Die Kategorie **Benachrichtigungen** weist einer Richtlinie Standardalarmbenachrichtigungen zu. **Jeder Benachrichtigungstyp hat andere Konfigurationseinstellungen**

(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#2187.htm).

Hinweis: Wenn mehrere Richtlinien demselben Rechner zugewiesen sind, werden alle zugewiesenen *Ereignisprotokoll-Benachrichtigungen* in allen zugewiesenen Richtlinien auf diesem Rechner bereitgestellt. Bei allen anderen Benachrichtigungstypen kann immer nur eine Richtlinie gleichzeitig gelten.

Hinweis: Im Feld der E-Mail-Empfänger für diese Benachrichtigungen können **Token** *(siehe 41)* verwendet werden.

- **Benachrichtigung hinzufügen**
  - Die Seite **Meldungen – Agent-Status** löst eine Meldung aus, wenn ein Agent offline ist, erstmals online geht, oder wenn jemand die Fernsteuerung des ausgewählten Rechners deaktiviert hat.
  - Die Seite **Meldungen – Anwendungsänderungen** löst eine Meldung aus, wenn auf ausgewählten Rechnern eine Anwendung installiert oder entfernt wird.
  - Die Seite **Meldungen – Dateien abrufen** löst eine Meldung aus, wenn der Befehl **getFile()** oder **getFileInDirectoryPath()** eines Verfahrens ausgeführt und nach dem Hochladen der Datei festgestellt wird, dass diese sich von der auf dem Kaseya Server gespeicherten Kopie unterscheidet. Liegt auf dem Kaseya Server keine vorherige Kopie vor, wird der Alarm erstellt.
  - Die Seite **Meldungen – Hardwareänderungen** löst eine Meldung aus, wenn sich die Hardwarekonfiguration auf den ausgewählten Rechnern ändert. Die ermittelten Hardwareänderungen umfassen das Hinzufügen oder Entfernen von RAM, PCI-Geräten und Plattenlaufwerken.
  - Die Seite **Meldungen – Geringer Plattenspeicher** löst eine Meldung aus, wenn der verfügbare Plattenspeicher unter einen vorgegebenen Prozentsatz des freien Plattenspeicherplatzes fällt.
  - Die Seite **Meldungen – Ereignisprotokolle** löst eine Meldung aus, wenn ein Ereignisprotokolleintrag für einen ausgewählten Rechner vorgegebenen Kriterien entspricht. Nach Auswahl des **Ereignisprotokolltyps** können Sie die durch den **Ereignissatz** und die **Ereigniskategorie** vorgegebenen Meldungsbedingungen filtern.
  - Die Seite **Alarme - LAN-Watch** arbeitet zusammen mit den Seiten **LAN-Watch** *(http://help.kaseya.com/webhelp/DE/KDIS/9000000/index.asp#1944.htm)*. **LAN-Watch** scannt das lokale LAN einer Rechner-ID und ermittelt neue Rechner und Geräte, die mit dem LAN des Rechners verbunden werden. Die Seiten **LAN-Watch** und **Alarme - LAN-Watch** können im Anschluss beide einen Alarm auslösen, wenn im LAN ein neuer Rechner oder ein neues Gerät ermittelt wird. Nur diese Seite **Alarme - LAN-Watch** kann jedoch beim Ermitteln eines neuen Rechners oder Geräts im LAN ein Ticket erstellen.
  - Die Seite **Meldungen – Fehlgeschlagene Agent-Verfahren** löst eine Meldung aus, wenn die Ausführung eines Agent-Verfahrens auf einem verwalteten Rechner fehlschlägt.
  - Die Seite **Meldungen – Schutzverletzung** löst eine Meldung aus, wenn eine Datei geändert wird oder eine Schutzverletzung auf einem verwalteten Rechner festgestellt wird.
  - Die Seite **Meldungen – Patch-Meldung** löst eine Meldung für Patch-Managementereignisse auf verwalteten Rechnern aus.
- **Benachrichtigung entfernen** – Entfernt eine ausgewählte Benachrichtigung.

Richtlinien – Registerkarte "Einstellungen" – Auditplan

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Auditplan''

Die Kategorie **Auditplan** weist einer Richtlinie Zeitpläne für **Letztes Audit, Basis-Audit und System-Audit** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#222.htm)* zu. Jeder Audittyp zeigt die gleichen drei Zeitplanoptionen an.

- **Planung bearbeiten** – Bearbeitet einen vorhandenen Auditplan. Planen Sie die einmalige oder periodische Ausführung einer Aufgabe. Bei jeder Art der Wiederholung (einmal, minütlich, stündlich, täglich, wöchentlich, monatlich) werden weitere verfügbare Optionen angezeigt. Periodische Zeitplanung bedeutet, dass Sie Start- und Endtermine für die Wiederholung einstellen müssen. Mögliche Optionen:
  - **Der Zeitplan wird auf der Zeitzone des Agent basieren (statt der des Servers).** – Wenn diese Option ausgewählt wird, legen die Zeiteinstellungen im Dialogfeld "Scheduler" anhand der lokalen Zeit des Agent-Rechners fest, wann die Aufgabe ausgeführt werden soll. Andernfalls beziehen sich die Zeitangeben auf die Serverzeit, die unter "System > Einstellungen" festgelegt ist. Übernimmt die Standardeinstellungen aus der Seite "System > Standardeinstellungen".
  - **Verteilungsfenster** – Plant die Aufgabe zu einem willkürlichen Zeitpunkt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen. Beispiel: Wenn die Ausführung einer Aufgabe für 3:00 Uhr geplant ist und das Verteilungsfenster 1 Stunde beträgt, wird die Zeitplanung für die Aufgabe in einen zufälligen Zeitpunkt zwischen 3:00 und 4:00 Uhr geändert.
  - **Überspringen, wenn offline** – Falls dies aktiviert und der Rechner offline ist, wird dies übergangen und zur nächsten geplanten Uhrzeit ausgeführt. Wenn diese Option leer gelassen wird und der Rechner offline ist, führen Sie die Aufgabe aus, sobald der Rechner wieder online ist.
  - **Bei offline einschalten** – Nur Windows. Wenn dies aktiviert ist, wird der Rechner hochgefahren, falls er offline ist. Erfordert Wake-On-LAN oder vPro und ein anderes verwaltetes System auf dem gleichen LAN.
  - **Folgenden Zeitrahmen ausschließen** – **Bezieht sich ausschließlich auf das Verteilungsfenster.** Falls markiert, wird ein Zeitrahmen im Verteilungsfenster angegeben, in dem die Aufgabe nicht geplant werden kann. Zeitangaben außerhalb des Verteilungsfensters werden ignoriert.
- **Zurücksetzen** – Für diesen Audittyp ist bei dieser Richtlinie kein Zeitplan eingestellt. Wenn für den gleichen Audittyp in einer Richtlinie mit niedrigerer Priorität ein Zeitplan definiert ist, so *darf* er wirksam werden.
- **Keine** – Für diesen Audittyp ist bei dieser Richtlinie kein Zeitplan eingestellt. Wenn für den gleichen Audittyp in einer Richtlinie mit niedrigerer Priorität ein Zeitplan definiert ist, so *darf er nicht* wirksam werden.

Richtlinien – Registerkarte "Einstellungen" – Anmeldung

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Anmeldung''

Die Kategorie **Anmeldung** weist einer Richtlinie Agent-**Anmeldungs** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#243.htm)*-Einstellungen zu.

Primärer KServer

Geben Sie die IP-Adresse oder den vollständig qualifizierten Hostnamen des primären Kaseya Server der Rechner-ID ein. Diese Einstellung wird in der Spalte **Primärer KServer** angezeigt.

Kaseya-Agents starten sämtliche Kommunikation mit Kaseya Server. Darum müssen die Agents immer den Domain-Namen oder die IP (Internetprotokoll)-Adresse erreichen, die Kaseya Server zugewiesen ist. Wählen Sie eine IP-Adresse oder einen Domänennamen, der von allen gewünschten Netzwerken (sowohl im lokalen LAN und im Internet) aus aufgelöst werden kann.

Best Practices: Obwohl eine öffentliche IP-Adresse verwendet werden kann, empfiehlt Kaseya die Verwendung eines **Domain Name Server (DNS)**-Namens für Kaseya Server. Dies wird als Vorsichtsmaßnahme empfohlen, falls die IP-Adresse geändert werden muss. Es ist einfacher, den DNS-Eintrag zu ändern, als verwaiste Agents umzuleiten.

Primärer Port

Geben Sie die Port-Nummer des primären Kaseya Server oder eines virtuellen Systemservers ein. Diese Einstellung wird in der Spalte **Primärer KServer** angezeigt.

Warnung: Verwenden Sie KEINEN *Computernamen* für Ihren Server. Der Agent verwendet standardmäß WinSock-Aufrufe, um einen vollständig qualifizierten Hostnamen in eine IP-Adresse aufzulösen, die für alle Agent-Verbindungen verwendet wird. Der Rechnername wird von NETBIOS in eine IP-Adresse aufgelöst. Dies ist eventuell nicht auf jedem Rechner aktiviert. NETBIOS ist eine optionale letzte Methode, die Windows zum Auflösen eines Namens einsetzt. Daher werden nur vollständig qualifizierte Namen oder IP-Adressen unterstützt.

Sekundärer KServer

Geben Sie die IP-Adresse oder den vollständig qualifizierten Hostnamen des sekundären Kaseya Serverder Rechner-ID ein. Diese Einstellung wird in der Spalte **Sekundärer KServer** angezeigt.

Sekundärer Port

Geben Sie die Port-Nummer des sekundären Kaseya Server oder eines virtuellen Systemservers ein. Diese Einstellung wird in der Spalte **Sekundärer KServer** angezeigt.

Check-in-Periode

Geben Sie das Zeitintervall ein, wie lange ein Agent warten soll, bis er einen Schnell-Check-in mit Kaseya Server durchführt. Eine Anmeldung nimmt eine Prüfung im Hinblick auf eine neue Aktualisierung des Rechner-ID-Kontos vor. Wenn eine neue Aktualisierung von einem VSA-Benutzer eingestellt wurde, beginnt der Agent mit der Aufgabe bei der nächsten Anmeldung. Diese Einstellung wird in der Spalte **Check-in-Periode** angezeigt. Die minimal und maximal zulässigen Check-in-Perioden werden über System > Anmelderichtlinie eingerichtet.

Best Practices: Der Agent erhält eine ständige Verbindung mit Kaseya Server aufrecht. Daher wirken sich Schnell-Check-in-Zeiten nicht auf die Reaktionszeiten des Agent aus. Die Schnell-Check-in-Zeit legt die maximale Wartezeit fest, bevor eine ausgefallene Verbindung wiederhergestellt wird. Die Einrichtung der Schnellanmeldung der Rechner auf 30 Sekunden garantiert, dass sich jeder Agent innerhalb von 30 Sekunden von einer ausgefallenen Verbindung erholt. Dabei wird vorausgesetzt, dass die Verbindung erfolgreich ist.

An Kserver binden

Bei Markierung ist der Agent an eine **eindeutige Kaseya Server-ID** gebunden. Gebundene Agents können erst dann einchecken, wenn die eindeutige Kaseya Server-ID, an die sie über "Agent > Check-in-Kontrolle" gebunden wurden, der eindeutigen ID des Kaseya Server unter "System > Konfigurieren > **ID ändern**" entspricht. Dadurch wird das Spoofing der IP-Adresse durch Umleitung von

Agent-Check-ins verhindert. Ein Schloss-symbol im Seitenbereich zeigt, dass der Agent gebunden ist. Um Agents zu *lösen*, wählen die Rechner-IDs aus, entfernen das Häkchen bei **An Kserver binden** und klicken auf **Aktualisieren**. Das Schloss-symbol wird die ausgewählten Rechner nicht mehr angezeigt.

Bandbreitenkontrolle

Mit dieser Funktion beschränken Sie den Agent auf den Verbrauch einer Höchstmenge an Bandbreite im System. Standardmäßig teilt sich der Agent die Bandbreite mit allen anderen laufenden Anwendungen, sodass normalerweise keine Bandbreitenkontrolle aktiviert werden muss. Deaktivieren Sie die Bandbreitenkontrolle, indem Sie eine 0 eingeben.

Warnen, wenn mehrere Agents das gleiche Konto verwenden

Der Kaseya Server kann ermitteln, wenn mehr als ein Agent eine Verbindung mit Kaseya Server herstellt und dieselbe ID.group ID.Organization ID-ID verwendet. Dieses Problem kann durch das Installieren eines Agent-Installationspakets aufgetreten sein, das mit der gleichen Rechner-ID auf mehr als einem Rechner vorkonfiguriert wurde. Markieren Sie dieses Kontrollkästchen, um jedes Mal, wenn Sie sich als Benutzer Kaseya Server anmelden, Benachrichtigungen über mehrere Agents zu erhalten, die dasselbe Konto verwenden.

Warnen, wenn Agent im selben LAN wie KServer über ein Gateway verbunden ist

Wenn Sie Rechner verwalten, die das gleiche LAN nutzen wie Ihr Kaseya Server, erhalten Sie möglicherweise diese Benachrichtigung Standardgemäß verbinden sich alle Agents zurück zum Kaseya Server mit dem externen Namen/IP-Adresse. TCP/IP-Meldungen dieser Agents werden über Ihr internes LAN an Ihren Router und anschließend zurück zum Kaseya Server geleitet. Einige Router leiten internen Verkehr mehr schlecht als recht durch sich selbst zurück. Markieren Sie dieses Kontrollkästchen, um eine Meldung zu erhalten, wenn der Kaseya Server einen Agent im selben LAN ermittelt, der aber über den Router verbunden ist.

Hinweis: Agents im selben LAN wie der Kaseya Server sollten die gemeinsame interne IP-Adresse des Agent und des Kaseya Server angeben, die auf der Seite Check-in-Kontrolle festgelegt wurde.

Richtlinien – Registerkarte "Einstellungen" – Anmeldedaten

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Anmeldedaten''

Die Kategorie **Anmeldedaten** weist einer Richtlinie **Anmeldedaten** *(siehe 37)* zu. *Bei vielen Richtlinien sind Agent-Anmeldeinformationen zum erfolgreichen Ausführen erforderlich.*

Warnung: **Policy Management** ignoriert Agent-Anmeldeinformationen, die über die Seite Agent > **Anmeldedaten eingeben** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#352.htm)* angegeben wurden.

- **Verwaltete Anmeldedaten verwenden** – **Bei Markierung müssen Anmeldedaten für alle Unternehmen oder Rechner eingegeben werden, denen diese Richtlinie zugewiesen wird, über die Seite Audit > Anmeldeinformationen verwalten (http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#11364.htm).**
- **Benutzername** – Geben Sie den Benutzernamen für die Anmeldeinformationen ein. Normalerweise ist dies ein Benutzerkonto.
- **Kennwort** – Geben Sie das Kennwort ein, das mit dem oben genannten Benutzernamen verknüpft ist.
- **Domäne**

- **Lokales Benutzerkonto** – Wählen Sie diese Option aus, um Anmeldeinformationen für eine lokale Anmeldung an diesem Rechner ohne Verweis auf eine Domäne zu verwenden.
- **Aktuelle Domäne des Rechners verwenden** – Erstellen Sie Anmeldeinformationen unter Verwendung des Namens der Domäne, deren Mitglied dieser Rechner ist. Dies wird vom letzten Audit bestimmt. **Alles markieren** erlaubt schnell und einfach einen gemeinsamen Benutzernamen / ein gemeinsames Kennwort auf mehreren Rechnern einzurichten, selbst wenn ausgewählte Rechner verschiedenen Domänen angehören.
- **Domäne angeben** – Geben Sie den Domänennamen manuell an, der für diese Anmeldeinformationen verwendet werden soll.

Richtlinien – Registerkarte "Einstellungen" – Datei verteilen

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Datei verteilen''

Die Kategorie **Datei verteilen verteilt Dateien** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#392.htm)*, die auf Kaseya Server gespeichert sind, auf Rechnern, denen diese Richtlinie zugewiesen ist.

Hinweis: Dieses Richtlinienobjekt **Datei verteilen** ist nicht in einem **SaaS** *(siehe 40)*-basierten VSA verfügbar.

Serverdatei auswählen

Wählen Sie eine Datei aus, die an verwaltete Rechner verteilt werden soll. Dies ist derselbe Dateisatz, der durch Klicken auf den Link **Dateien verwalten...** auf dieser Seite verwaltet wird.

Hinweis: Es werden nur Ihre eigenen persönlichen verwalteten Dateien oder freigegebene verwaltete Dateien angezeigt. Sollte ein anderer Benutzer eine persönliche Datei verteilen, können Sie diese nicht sehen.

Legen Sie den vollständigen Pfad und Dateinamen fest, um die Datei auf dem Remote Rechner zu speichern

Geben Sie den Pfad und Dateinamen ein, um diese Datei auf ausgewählten Rechner-IDs zu speichern.

Richtlinien – Registerkarte "Einstellungen" – Ereignisprotokolleinstellungen

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Ereignisprotokolleinstellungen''

Die Kategorie **Ereignisprotokolleinstellungen** gibt die **Ereignisprotokolltypen und -kategorien** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#3713.htm)* an, die zur Angabe von Ereignisprotokoll-Benachrichtigungen verwendet werden.

So legen Sie **Ereignisprotokolleinstellungen** fest:

1. Klicken Sie auf einen Ereignisprotokolltyp im Listenfeld **Verfügbar**. Halten Sie die [Strg]-Taste gedrückt, um mehrere Ereignisprotokolltypen auszuwählen.

2. Klicken Sie auf **>**, um dem Listenfeld **Ausgewählt** Ereignisprotokolltypen hinzuzufügen. Klicken Sie auf **<** , um Ereignisprotokolltypen aus dem Listenfeld **Ausgewählt** zu entfernen.
3. Markieren Sie eine oder mehrere Ereigniskategorien:
   - **Fehler**
   - **WARNUNG**
   - **Informationen**
   - **Erfolgs-Audit**
   - **Fehler-Audit**
   - **Kritisch** – Betrifft nur Vista, Windows 7 und Windows Server 2008
   - **Ausführlich** – Betrifft nur Vista, Windows 7 und Windows Server 2008

Richtlinien – Registerkarte "Einstellungen" – Kaseya AntiMalware

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kaseya AntiMalware Kontrollkästchen

Die Kategorie **Kaseya AntiMalware** weist einem **AntiMalware Profil** *(http://help.kaseya.com/webhelp/DE/KAM/9000000/index.asp#7322.htm)* eine Richtlinie zu. Auf Rechnern, denen diese Richtlinie zugewiesen ist, muss bereits der **AntiMalware**-Client installiert sein.

- **Profil** – Wählt das **AntiMalware**-Profil aus, das dieser Richtlinie zugewiesen werden soll.

Richtlinien – Registerkarte "Einstellungen" – Kaseya Antivirus

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kaseya Antivirus Kontrollkästchen

Die Kategorie **Kaseya Antivirus** weist einem **Antivirus Profil** *(http://help.kaseya.com/webhelp/DE/KAV/9000000/index.asp#6837.htm)* eine Richtlinie zu. Auf Rechnern, denen diese Richtlinie zugewiesen ist, muss bereits der **Antivirus**-Client installiert sein. **Antivirus**weist automatisch den entsprechenden Profiltyp, Server oder Arbeitsplatzrechner, für einen Rechner zu.

- **Serverprofil** – Wählt das **Antivirus**-Serverprofil aus, das dieser Richtlinie zugewiesen werden soll.
- **Workstation-Profil** – Wählt das **Antivirus**-Workstation-Profil aus, das dieser Richtlinie zugewiesen werden soll.

Richtlinien – Registerkarte "Einstellungen" – Kaseya Security

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Kaseya Security''

Die Kategorie **Sicherheit** weist einem **Endpoint Security Profil** *(http://help.kaseya.com/webhelp/DE/KES/9000000/index.asp#2945.htm)* eine Richtlinie zu. Auf Rechnern, denen diese Richtlinie zugewiesen ist, muss bereits der **Endpoint Security**-Client installiert sein.

- **Profil** – Wählt das **Endpoint Security**-Profil aus, das dieser Richtlinie zugewiesen werden soll.

Richtlinien – Registerkarte "Einstellungen" – LAN-Cache

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''LAN-Cache''

Die Kategorie **LAN-Cache** weist einem **LAN-Cache** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#9328.htm)* eine Richtlinie zu.

- **LAN-Cache** – Wählt den LAN-Cache aus, der dieser Richtlinie zugewiesen werden soll.

Richtlinien – Registerkarte "Einstellungen" – Protokollhistorie

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Protokollhistorie''

Die Kategorie **Protokollhistorie** weist **Protokollhistorieeinstellungen** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#238.htm)* einer Richtlinie zu.

Anzahl Tage festlegen, die Protokolleinträge aufbewahrt werden sollen. Markieren, um Einträge in Datei zu archivieren

Legen Sie die Anzahl der Tage fest, für die Protokolleinträge für jede Art von Protokoll aufbewahrt werden sollen. Aktivieren Sie das Kontrollkästchen für jedes Protokoll, um Protokolldateien nach ihrem Enddatum zu archivieren.

- **Konfigurationsänderungen** – Protokoll der von jedem Benutzer vorgenommenen Konfigurationsänderungen.
- **Netzwerkstatistiken** – Protokoll der ein- und ausgehenden Paketzahlinformationen und der Anwendung oder des Prozesses, die/der solche Pakete überträgt und/oder empfängt. Die Informationen können im Detail über Agent > Agent-Protokolle > Netzwerk-Statistik angezeigt werden.
- **Agent-Verfahrensprotokoll** – Protokoll der erfolgreichen/fehlgeschlagenen Agent-Verfahren.
- **Fernsteuerungsprotokoll** – Protokoll der Fernsteuerungsereignisse.
- **Alarmprotokoll** – Protokoll aller ausgegebener Alarme.
- **Vorgang überwachen** – Das Protokoll der aufgetretenen Alarmbedingungen sowie die entsprechenden Aktionen, die als Reaktion darauf ergriffen wurden.
- **SYS-Protokoll** – Das Protokoll aller Systemkontrollen externer Systeme.
- **Agent-Betriebszeitprotokoll** – Das Protokoll der Betriebszeit-Historie von Agents.

Festlegen, wie viele Tage die Monitor-Protokolle für alle Rechner aufbewahrt werden sollen

Die folgenden Monitoring-Protokolleinstellungen werden systemweit angewendet.

- **Ereignisprotokoll** – Protokoll aller Ereignisse. Die erfassten Ereignisse werden detaillierter über Agent > Ereignisprotokolleinstellungen angegeben.
- **Monitoring-Protokoll** – Protokoll der von Monitor-Sets erfassten Daten
- **SNMP-Protokoll** – Protokoll aller von SNMP-Sets erfassten Daten.
- **Agent-Protokoll** – Protokoll der Agent-, System- und Fehlermeldungen

Richtlinien – Registerkarte "Einstellungen" – Rechnerprofil

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Rechnerprofil''

Die Kategorie **Rechnerprofil** weist einer Richtlinie **Rechnerprofil** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#256.htm)*-Einstellungen zu.

- **Kontaktname** – Geben Sie den Namen der Person ein, die den verwalteten Rechner benutzt. Diese Einstellung wird in der Spalte **Kontaktname** angezeigt.
- **Kontakt-E-Mail** – Geben Sie die E-Mail-Adresse der Person ein, die den verwalteten Rechner benutzt. Diese Einstellung wird in der Spalte **Kontakt-E-Mail** angezeigt.
- **Kontakt Telefon** – Geben Sie die Telefonnummer der Person ein, die den verwalteten Rechner benutzt. Diese Einstellung wird in der Spalte **Kontakt-Telefon** angezeigt.
- **E-Mail-Administrator** – Geben Sie die E-Mail-Adresse für Administrator-Support bei diesem verwalteten Rechner ein. Diese Einstellung wird in der Spalte **E-Mail-Administrator** angezeigt.
- **Spracheinstellungen** – Die in der Dropdown-Liste **Spracheinstellungen** ausgewählte Sprache legt die Sprache fest, die in einem Agent-Menü auf einem verwalteten Rechner angezeigt wird. Die verfügbaren Sprachen werden von den über System > Voreinstellungen installierten Sprachpaketen bestimmt.
- **Rechnerrolle** – Die Rechnerrolle, die auf ausgewählte Rechner-IDs angewendet wird. Rechnerrollen legen die Funktionen für den Portalzugriff fest, die dem Rechnerbenutzer zur Verfügung stehen.
- **Anmerkungen** – Geben Sie Anmerkungen zu einem Rechner-ID-Konto ein. Hilfreiche Daten sind zum Beispiel Standort des Rechners, Rechnertyp, Firma oder sonstige Erkennungsdaten zum verwalteten Rechner.
- **Anmerkungen als Quickinfo anzeigen** – Wenn **Profil bearbeiten** aktiviert ist, werden Anmerkungen als Teil der Quickinfo ergänzt, die angezeigt werden, wenn der Cursor über das Anmeldestatussymbol einer Rechner-ID fährt.
- **Tickets automatisch zuweisen** – Weisen Sie dieser Rechner-ID automatisch ein Ticket zu, wenn der **Ticketing** E-Mail-Reader eine E-Mail-Nachricht von derselben E-Mail-Adresse wie die **Kontakt-E-Mail** erhält. Dies trifft zu, wenn neue E-Mail-Nachrichten in den Ticket-E-Mail-Reader eingehen, die keiner E-Mail-Zurordnung zugeordnet werden können.

> **Hinweis:** wenn mehrere Rechner-IDs die gleiche Kontakt-E-Mail haben, kann das Kontrollkästchen **Tickets automatisch zuweisen** nur bei einem einzigen Rechner aktiviert sein.

Richtlinien – Registerkarte "Einstellungen" – Monitor-Sets

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Monitor-Sets''

Die Kategorie **Monitor-Sets** weist einer Richtlinie **Monitor-Sets** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#1938.htm)* zu.

> **Hinweis:** Wenn mehrere Richtlinien demselben Rechner zugewiesen sind, werden alle zugewiesenen Monitor-Sets in allen zugewiesenen Richtlinien auf diesem Rechner bereitgestellt.

- **Monitor-Set hinzufügen** – Weist Monitor-Sets zu und plant sie. Markieren Sie beliebige dieser Kontrollkästchen, um bei Auftreten einer Alarmbedingung die entsprechenden Aktionen auszuführen.
  - **Alarm erstellen**
  - **Ticket erstellen**
  - **Skript** `<agentprocedure>` ausführen auf `<machineID>`
  - **E-Mail-Empfänger** – Geben Sie mehrere Adressen durch Kommas getrennt ein.

    Hinweis: In diesem Feld können **Token** *(siehe 41)* verwendet werden.
- **Monitor-Set entfernen** – Entfernt ein ausgewähltes Agent-Verfahren.

Richtlinien – Registerkarte "Einstellungen" – Patchdateiquelle

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Patchdateiquelle''

Die Kategorie **Patchdateiquelle** definiert anhand der Richtlinie die **Dateiquelle** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#366.htm)* für mit Patch ausführbare Dateien.

- **Pakete ins Arbeitsverzeichnis auf dem Laufwerk mit dem meisten freien Speicherplatz kopieren** – Patches werden auf die Festplatte des lokal verwalteten Rechners heruntergeladen oder von einer Dateifreigabe kopiert. Für die komplette Installation mehrerer Patches und insbesondere Service Packs wird möglicherweise bedeutend mehr freier Speicherplatz auf der lokalen Festplatte benötigt. Aktivieren Sie dieses Kontrollkästchen, um Patches in das Arbeitsverzeichnis herunterzuladen herunterzuladen, hierbei jedoch das Laufwerk auf dem verwalteten Rechner mit dem meisten freien Speicherplatz zu verwenden. Deaktivieren Sie dieses Kontrollkästchen, wenn immer das im **Arbeitsverzeichnis** für die Rechner-ID angegebene Laufwerk verwendet werden soll.
- **Paket nach der Installation löschen (aus dem Arbeitsverzeichnis)** – Das Installationspaket wird normalerweise nach Abschluss der Installation gelöscht, um wieder Speicherplatz freizugeben. Deaktivieren Sie dieses Kontrollkästchen, wenn das Paket zur Fehlersuche auf dem Computer belassen werden soll. Falls die Installation fehlschlägt und Sie die Befehlszeilen-Switches überprüfen müssen, sollten Sie das Paket nicht löschen, damit es Ihnen für Testzwecke zur Verfügung steht. Das Paket wird im **Arbeitsverzeichnis** auf dem in der vorherigen Option angegebenen Laufwerk gespeichert.
- **Aus dem Internet herunterladen** – Jeder verwaltete Rechner lädt die ausführbare Patch-Datei direkt vom Internet unter der in Patch-Speicherort angegebenen URL herunter.
- **Vom Systemserver eingeholt** – Zunächst prüft der Kaseya Server, ob er bereits eine Kopie der Patch-Datei besitzt. Wenn nicht, wird die neue ausführbare Patch-Datei automatisch heruntergeladen und auf dem Kaseya Server gespeichert. Sie wird anschließend für alle weiteren Verteilungen auf verwaltete Rechner verwendet. Wenn ein Patch auf einem verwalteten Rechner installiert werden muss, wird diese Patch-Datei von Kaseya Server auf diesen Rechner übertragen.

  Hinweis: Der Speicherort der auf dem Kaseya Server gespeicherten Patch-Dateien ist `<Kaseya installation directory>\WebPages\ManagedFiles\VSAPatchFiles\`
- **Vom Dateiserver über UNC-Pfad geladen** – Diese Methode wird empfohlen, wenn Sie zahlreiche Rechner im gleichen LAN unterstützen. Patch-Dateien werden in ein lokales Verzeichnis auf einer ausgewählten Rechner-ID heruntergeladen. Das lokale Verzeichnis auf der Rechner-ID wird zur gemeinsamen Verwendung mit anderen Rechner-IDs im gleichen LAN konfiguriert. Alle anderen Rechner-IDs im gleichen LAN verwenden einen UNC-Pfad zu dem freigegebenen Ordner auf der ersten Rechner-ID.

1. Geben Sie einen *Agent-Rechner* an, der als *Dateiserverrechner* für andere Rechner im selben LAN dienen soll.
2. Erstellen Sie eine Freigabe auf dem *Dateiserverrechner* und geben Sie die Anmeldedaten an, mit denen andere Rechner im selben LAN darauf zugreifen können. Dies geschieht manuell, nicht auf der Seite **Dateiquelle**.
3. Stellen Sie Anmeldedaten für den *Dateiserverrechner* mit dem freigegebenen Verzeichnis mithilfe von Agent > Anmeldedaten eingeben ein. Alle anderen Rechner im selben LAN verwenden den Anmeldedatensatz für den *Dateiserverrechner*, um auf den freigegebenen Ordner zuzugreifen.
4. Geben Sie einen freizugebenden UNC-Pfad in das Feld **Vom Dateiserver über UNC-Pfad geladen** ein. Zum Beispiel `\\computername\sharedname\dir\`.

In den nächsten drei Schritten teilen Sie VSA mithilfe der lokalen Dateiformat-Schreibweise mit, welche Rechner-ID als *Dateiserverrechner* dient und wo sich das freigegebene Verzeichnis befindet.

5. Anhand der Dropdown-Liste **Rechner-Gruppenfilter** können Sie eine Gruppen-ID auswählen.
6. Wählen Sie eine Rechner-ID aus der Dropdown-Liste **Dateifreigabe befindet sich auf** aus.
7. Geben Sie im Feld **im lokalen Verzeichnis** ein gemeinsames lokales Verzeichnis ein.

> **Hinweis:** Der Wert im Feld **im lokalen Verzeichnis** muss mit dem vollständigen Pfad eingegeben werden, z. B. `c:\shareddir\dir`.

Wenn eine Datei heruntergeladen wird, prüft der Kaseya Server zunächst, ob sich die Patch-Datei bereits in der Dateifreigabe befindet. Wenn nicht, lädt der *Dateiserverrechner* die Patch-Datei automatisch entweder direkt vom Internet herunter oder ruft sie vom Kaseya Server ab.

8. **Der Dateiserver erhält die Patchdateien automatisch vom** – Wählen Sie eine der folgenden Optionen aus:
   - ✓ **das Internet** – Verwenden Sie diese Einstellung, wenn der *Dateiserverrechner* vollen Internetzugriff hat.
   - ✓ **der Systemserver** – Verwenden Sie diese Einstellung, wenn der Internetzugriff des *Dateiserverrechners* blockiert ist.
9. **Aus dem Internet herunterladen, wenn der Rechner keine Verbindung zum Dateiserver herstellen kann** – Aktivieren Sie wahlweise dieses Kontrollkästchen, um vom Internet herunterzuladen. Dies ist in erster Linie für Laptops geeignet, die zwar vom Firmennetzwerk getrennt sind, jedoch Internetzugriff haben.

- **Geladen von LAN-Cache** – Verwendet die Seiten Agent > LAN-Cache und Agent > LAN-Cache zuweisen, um Dateiquellen für ausführbare Patch-Dateien zu verwalten.

Richtlinien – Registerkarte "Einstellungen" – Patch-Verfahren-Planung

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Patch-Verfahren-Planung''

Die Kategorie **Patch-Verfahren-Planung** plant zwei Aufgaben, die einer Richtlinie zugewiesen werden können.

- **Patch-Scan** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#350.htm)* – Plant Scans, um auf jedem verwalteten Rechner nach fehlenden Patches zu suchen. Der Scanvorgang ist nicht ressourcenintensiv, und er kann problemlos zu jeder Tageszeit geplant werden. Die Benutzer werden durch den Scanvorgang in keinster Weise gestört.

- **Automatisches Update** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#348.htm)* – Plant ein Update verwalteter Rechner mit Microsoft-Patches in *wiederkehrenden* Zyklen. **Automatische Aktualisierung** unterliegt sowohl der **Patch-Bestätigungsregel** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#3873.htm)* als auch der **Richtlinien – Registerkarte "Einstellungen" – Patch-Neustart-Aktion** *(siehe 21)*-Regel

Patch-Scan und **Automatisches Update** zeigen beide die gleichen drei Optionen an und können innerhalb derselben Richtlinie separat eingestellt werden.

- **Planung bearbeiten** – Bearbeitet einen vorhandenen Aufgabenplan. Planen Sie die einmalige oder periodische Ausführung einer Aufgabe. Bei jeder Art der Wiederholung (einmal, minütlich, stündlich, täglich, wöchentlich, monatlich) werden weitere verfügbare Optionen angezeigt. Periodische Zeitplanung bedeutet, dass Sie Start- und Endtermine für die Wiederholung einstellen müssen. Mögliche Optionen:
  - **Der Zeitplan wird auf der Zeitzone des Agent basieren (statt der des Servers).** – Wenn diese Option ausgewählt wird, legen die Zeiteinstellungen im Dialogfeld "Scheduler" anhand der lokalen Zeit des Agent-Rechners fest, wann die Aufgabe ausgeführt werden soll. Andernfalls beziehen sich die Zeitangeben auf die Serverzeit, die unter "System > Einstellungen" festgelegt ist. Übernimmt die Standardeinstellungen aus der Seite "System > Standardeinstellungen".
  - **Verteilungsfenster** – Plant die Aufgabe zu einem willkürlichen Zeitpunkt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen. Beispiel: Wenn die Ausführung einer Aufgabe für 3:00 Uhr geplant ist und das Verteilungsfenster 1 Stunde beträgt, wird die Zeitplanung für die Aufgabe in einen zufälligen Zeitpunkt zwischen 3:00 und 4:00 Uhr geändert.
  - **Überspringen, wenn offline** – Falls dies aktiviert und der Rechner offline ist, wird dies übergangen und zur nächsten geplanten Uhrzeit ausgeführt. Wenn diese Option leer gelassen wird und der Rechner offline ist, führen Sie die Aufgabe aus, sobald der Rechner wieder online ist.
  - **Bei offline einschalten** – Nur Windows. Wenn dies aktiviert ist, wird der Rechner hochgefahren, falls er offline ist. Erfordert Wake-On-LAN oder vPro und ein anderes verwaltetes System auf dem gleichen LAN.
  - **Folgenden Zeitrahmen ausschließen** – **Bezieht sich ausschließlich auf das Verteilungsfenster.** Falls markiert, wird ein Zeitrahmen im Verteilungsfenster angegeben, in dem die Aufgabe nicht geplant werden kann. Zeitangaben außerhalb des Verteilungsfensters werden ignoriert.
- **Zurücksetzen** – Für diese Aufgabe ist bei dieser Richtlinie kein Zeitplan eingestellt. Wenn für die gleiche Aufgabe in einer Richtlinie mit niedrigerer Priorität ein Zeitplan definiert ist, so *darf* er wirksam werden.
- **Keine** – Für diese Aufgabe ist bei dieser Richtlinie kein Zeitplan eingestellt. Wenn für die gleiche Aufgabe in einer Richtlinie mit niedrigerer Priorität ein Zeitplan definiert ist, so *darf er nicht* wirksam werden.

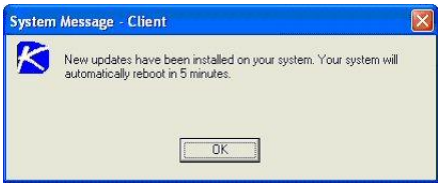
Richtlinien – Registerkarte "Einstellungen" – Patch-Neustart-Aktion

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Patch-Neustart-Aktion''

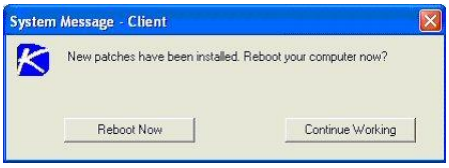
Die Richtlinienkategorie **Patch-Neustart-Aktion** weist einer Richtlinie eine **Neustart-Aktion** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#358.htm)* für mit Patch ausführbare Dateien zu.

- **Neustart sofort nach Aktualisierung** – Startet den Rechner unmittelbar nach dem Abschluss der Installation neu.

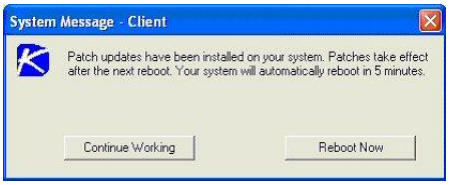
- **Neu starten am <Wochentag> um <Uhrzeit> nach Installation** – Nach Abschluss der Patch-Installation wird der Rechner an dem ausgewählten Wochentag zu der angegebenen Uhrzeit neu gestartet. Anhand dieser Einstellungen können Sie Patches tagsüber installieren, wenn Benutzer angemeldet sind, und dann nachts einen Neustart erzwingen. Wenn **jeden Tag** ausgewählt ist, wird der Rechner zum angegebenen Zeitpunkt nach Abschluss der Patch-Installation neu gestartet.
- **Benutzer warnen, dass der Rechner in <N> Minuten neu startet (ohne Anfrage auf Genehmigung)** – Wenn eine Patch-Installation abgeschlossen ist, wird die nachstehende Meldung angezeigt, die den Benutzer warnt und ihm die angegebene Anzahl von Minuten anzeigt, um seinen aktuellen Arbeitsschritt abzuschließen und seine Arbeit zu speichern. Falls niemand angemeldet ist, startet das System sofort neu.


System Message - Client
New updates have been installed on your system. Your system will automatically reboot in 5 minutes.
OK

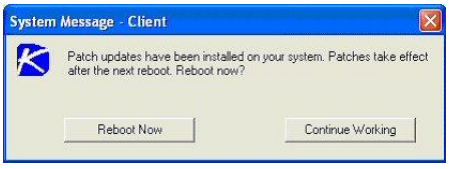
- **Neustart übergehen, falls Benutzer angemeldet ist** – Wenn der Benutzer angemeldet ist, wird der Neustart nach Abschluss der Patch-Installation übergangen. Verwenden Sie diese Einstellung, um eine Störung der Benutzer zu vermeiden. Dies ist die Standardeinstellung.
- **Falls der Benutzer angemeldet, Neustart anfragen alle <N> Minuten bis zum Neustart** – Bei dieser Einstellung wird die nachstehende Meldung angezeigt, in der der Benutzer gefragt wird, ob jetzt ein Neustart durchgeführt werden kann. Wenn sich niemand am Computer befindet oder der Benutzer mit 'Nein' antwortet, wird die gleiche Meldung alle N Minuten angezeigt, bis das System neu gestartet wird. Falls niemand angemeldet ist, startet das System sofort neu.



- **Um Erlaubnis fragen, falls der Benutzer angemeldet ist. Neu starten, wenn keine Antwort erfolgt nach <N> Minuten. Neustart, wenn der Benutzer nicht angemeldet ist** – Bei dieser Einstellung wird die nachstehende Meldung angezeigt, in der der Benutzer gefragt wird, ob jetzt ein Neustart durchgeführt werden kann. Falls sich niemand am Computer befindet, wird dieser automatisch nach N Minuten gestartet, **ohne dass offene Dokumente gespeichert werden**. Falls niemand angemeldet ist, startet das System sofort neu.


System Message - Client
Patch updates have been installed on your system. Patches take effect after the next reboot. Your system will automatically reboot in 5 minutes.
Continue Working
Reboot Now

- **Um Erlaubnis fragen, falls der Benutzer angemeldet ist. Keine Aktion, wenn keine Antwort erfolgt nach <N> Minuten. Neustart, wenn der Benutzer nicht angemeldet ist** – Bei dieser Einstellung wird die nachstehende Meldung angezeigt, in der der Benutzer gefragt wird, ob jetzt ein Neustart durchgeführt werden kann. Wenn sich niemand am Computer befindet, wird der Neustart übergangen. Falls niemand angemeldet ist, erfolgt sofort ein Neustart.


System Message - Client
Patch updates have been installed on your system. Patches take effect after the next reboot. Reboot now?
Reboot Now
Continue Working

- **Nicht neu starten nach Aktualisierung** – Startet nicht neu. Diese Einstellung wird in der Regel für Server verwendet, bei denen der Neustart kontrolliert durchgeführt werden muss. Sie können per E-Mail benachrichtigt werden, wenn ein neuer Patch installiert wurde. Hierfür aktivieren Sie **E-Mail senden, wenn Neustart erforderlich** und geben Sie eine E-Mail-Adresse ein.

Richtlinien – Registerkarte "Einstellungen" – Patch-Einstellungen

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Patch-Einstellungen''

Die Kategorie **Patch-Einstellungen** weist einer Richtlinie Patch-Einstellungen zu.

Vor-/Nach-Verfahren *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#2210.htm)*

Führen Sie Verfahren entweder vor und/oder nach dem **ersten Update** oder dem **automatischen Update** aus. Sie können beispielsweise Verfahren ausführen, die die Vorbereitung und Einrichtung neu hinzugefügter Rechner vor oder nach einer **Eingangsaktualisierung** automatisieren.

- **Verfahren vor dem Initial Update ausführen**
- **Verfahren nach dem Initial Update ausführen**
- **Verfahren vor automatischem Update ausführen**
- **Verfahren nach automatischem Update ausführen**

Zugehörigkeit zu Patch-Richtlinie *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#218.htm)*

Weisen Sie dieser Richtlinie einen oder mehrere Patch-Richtliniennamen zu.

Patch-Benachrichtigung *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#2889.htm)*

Markieren Sie beliebige dieser Kontrollkästchen, um bei Auftreten einer Alarmbedingung die entsprechenden Aktionen auszuführen.

- **Alarm erstellen**
- **Ticket erstellen**
- **Skript** `<agentprocedure>` ausführen auf `<machineID>`
- **E-Mail-Empfänger** – Geben Sie mehrere Adressen durch Kommas getrennt ein.

> **Hinweis:** In diesem Feld können **Token** *(siehe 41)* verwendet werden.

Das System kann einen Alarm bei den folgenden Alarmbedingungen für eine ausgewählte Rechner-ID auslösen:

- **Neues Patch ist verfügbar**
- **Patch-Installation schlägt fehl**
- **Agent-Anmeldedaten sind ungültig oder fehlen**

> **Hinweis:** Agent-**Anmeldedaten** *(siehe 37)* sind für die Installation von Patches nicht erforderlich, **es sei denn**, die Dateiquelle des Rechners ist als `Pulled from file server using UNC path` konfiguriert. Wenn Agent-Anmeldeinformationen zugewiesen werden, werden sie als lokale Rechneranmeldeinformationen validiert, ungeachtet der **Dateiquellen**-Konfiguration. Wenn diese Validierung fehlschlägt, wird ein Alarm ausgelöst. Wenn die **Dateiquelle** des Rechners als `Pulled from file server using UNC path` konfiguriert wird, sind Anmeldedaten erforderlich. Wenn sie fehlen, wird ein Alarm ausgelöst. Falls die Anmeldedaten vorliegen, werden sie als Anmeldedaten für einen lokalen Rechner und als Anmeldedaten für ein Netzwerk validiert. Wenn eine dieser Validierungen fehlschlägt, wird ein Alarm ausgelöst.

- **Automatisches Windows Update geändert**

Richtlinien – Registerkarte "Einstellungen" – Automatische Windows-Aktualisierung patchen

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Automatische Windows-Aktualisierung patchen''

Die Kategorie **Automatische Windows-Aktualisierung patchen** weist die folgenden Richtlinien zu:

- **Deaktivieren Sie das automatische Windows Update, damit das Patch-Management die Steuerung des System-Patchings übernehmen kann** – Markieren Sie diese Option, um **Automatische Windows-Aktualisierung** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#2070.htm)* auf ausgewählten Rechner-IDs zu deaktivieren und die Anwendung von Patches auf dem verwalteten Rechner über **Patch-Verwaltung** zu steuern. Überschreibt die vorhandenen Benutzereinstellungen und deaktiviert die Kontrollen in Automatische Windows-Aktualisierung, sodass der Benutzer *keine* Einstellungen ändern kann. Benutzer können weiterhin manuell Patches auf ihre Systeme anwenden.

Richtlinien – Registerkarte "Einstellungen" – Schutz

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Schutz''

Die Kategorie **Schutz** weist einer Richtlinie Datei-, Anwendungs- und Netzwerkzugriff zu.

Dateizugriffsteuerung *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#405.htm)*

- **Datei hinzufügen** oder **Zugang ändern – Weist Monitor-Sets** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#1938.htm)* zu und plant sie. Markieren Sie beliebige dieser Kontrollkästchen, um bei Auftreten einer Alarmbedingung die entsprechenden Aktionen auszuführen.
  - **Dateiname für Zugriffskontrolle (voller Pfad erforderlich)** – Geben Sie den vollständigen Pfad- und Dateinamen ein.
  - **Anwendung mit Zugriffsbestätigung eingeben** – Fügen Sie eine neue Anwendung zu der Zugriffsliste hinzu.
  - **Bestätigte Anwendungen** – Zeigt die Liste der Anwendungen mit Zugriffsbestätigung ein
  - **Entfernen** – Entfernt eine ausgewählte Anwendung aus der Zugriffsbestätigungsliste.
  - **Benutzer fragen, die nicht aufgelisteten freizugeben** – Damit wird dem Benutzer die Möglichkeit gegeben, den Zugriff auf die Datei auf Anwendungsbasis jedes Mal zu gewähren oder zu verweigern, wenn eine neue Anwendung versucht, auf diese Datei zuzugreifen. Anhand dieser Funktion können Sie die Zugriffsliste basierend auf der normalen Nutzung aufbauen.
  - **Alle nicht aufgelisteten ablehnen** – Blockiert alle Anwendungen vom Zugriff auf die Datei. Wählen Sie diese Option, wenn Sie sich nicht sicher sind, für welche Dateien Zugriff benötigt wird und für welche nicht.
- **Datei entfernen** – Entfernt ein ausgewähltes Agent-Verfahren.

Anwendungsblockierer *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#409.htm)*

So blockieren Sie das Ausführen einer Anwendung auf einem Rechner:

1. Geben Sie den Dateinamen der Anwendung in das Bearbeitungsfeld ein.

2. Klicken Sie auf die Schaltfläche **Hinzufügen** . Die blockierte Anwendung wird in der Liste **Zu blockierende Anwendung** angezeigt.

So heben Sie die Blockierung einer Anwendung auf einem Rechner wieder auf:

1. Geben Sie den Dateinamen der Anwendung in das Bearbeitungsfeld ein.
2. Klicken Sie auf die Schaltfläche **Entfernen**. Die Anwendung wird nicht mehr in der Liste **Zu blockierende Anwendung** angezeigt.

Netzwerkzugriff *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#407.htm)*

- **Benutzer benachrichtigen, wenn Anwendung geblockt ist** – Benutzer benachrichtigen, wenn eine geblockte Anwendung auf das Netzwerk zugreifen will. Anhand dieser Funktion können Sie die Zugriffsliste basierend auf der normalen Nutzung aufbauen. Auf diese Weise können Sie sehen, welche Anwendungen auf Ihrem System auf das Netzwerk zugreifen und wann. Der Rechnerbenutzer ist aufgefordert eine von vier Antworten zu wählen, wenn eine Anwendung geblockt ist:
  - **Immer** – Gewährt der Anwendung unbegrenzt den Zugriff auf das Netzwerk. Die Benutzer werden nicht erneut aufgefordert.
  - **Ja** – Der Anwendung wird der Zugriff auf das Netzwerk für die Dauer der Sitzung gewährt. Die Benutzer werden erneut aufgefordert.
  - **Nein** – Der Anwendung wird der Zugriff auf das Netzwerk für die Dauer der Sitzung verweigert. Die Benutzer werden erneut aufgefordert.
  - **Nie** – Verweigert der Anwendung immer den Zugriff auf das Netzwerk. Die Benutzer werden nicht erneut aufgefordert.
- **Treiber bei nächstem Neustart aktivieren/deaktivieren** – den Netzwerkzugriff-Protection-Treiber für einen Agent **Aktivieren/Deaktivieren**. Anwendungen, die den Windows TCP/IP-Stapel nicht auf normale Weise verwenden, können Konflikte mit diesem Treiber verursachen. Dies gilt insbesondere für ältere Anwendungen. **Der Agent kann keine Netzwerkstatistiken überwachen oder den Netzwerkzugriff blockieren, wenn der Treiber deaktiviert ist.** *Bei Windows-Rechnern, die mit einem älteren Betriebssystem als Vista laufen, wird ein aktivierter Rechner erst nach einem Neustart des Rechners aktiv.*
- **Nicht gelistete Aktion anwenden** – Bei einer nicht gelisteten Anwendung handelt es sich um eine Anwendung, für die der Zugriff auf das Netzwerk nicht ausdrücklich gewährt oder verweigert wurde. Geben Sie an, was unternommen werden soll, wenn eine nicht gelistete Anwendung versucht, auf das Netzwerk zuzugreifen.
  - **Benutzer bitten, die nicht gelisteten freizugeben** – Ein Bestätigungsdialogfeld wird angezeigt, wenn eine nicht gelistete Anwendung versucht, auf das Netzwerk zuzugreifen.
  - **Alle nicht gelisteten freigeben** – Der nicht gelisteten Anwendung wird der Zugriff auf das Netzwerk gewährt.
  - **Alle nicht gelisteten ablehnen** – Der nicht gelisteten Anwendung wird der Zugriff auf das Netzwerk verweigert, und die Anwendung wird auf dem verwalteten Rechner geschlossen.

Richtlinien – Registerkarte "Einstellungen" – Remote Control

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Remote Control''

Die Kategorie **Remote Control** weist einer Richtlinie Einstellungen der **Benutzerbenachrichtigung** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#2930.htm)* durch Remote Control zu.

- **Benutzerbenachrichtigungstyp auswählen**:

- **Automatische Kontrolle –** Dem Benutzer wird nichts mitgeteilt. Sie übernehmen sofort und automatisch die Kontrolle.
- **Warnung, falls der Benutzer angemeldet ist** – Es wird eine Benachrichtigung mit Warntext angezeigt. Der Warntext kann im Bearbeitungsfeld unterhalb dieser Option bearbeitet werden.
- **Um Erlaubnis fragen, falls der Benutzer angemeldet ist** – Fragen Sie den Benutzer, ob es in Ordnung ist, eine Fernsteuerungssitzung zu beginnen. Der Text dieser Frage kann im Bearbeitungsfeld unterhalb dieser Option bearbeitet werden. Die Fernsteuerung kann erst beginnen, wenn der Benutzer auf die Schaltfläche **Ja** klickt. Wenn nach einer Minute keine Option angeklickt wurde, wird **Nein** angenommen und VSA entfernt das Dialogfeld vom Zielrechner. Wenn kein Benutzer angemeldet ist, fahren Sie mit der Fernsteuerungssitzung fort.
- **Erlaubnis erforderlich. Verweigert, falls niemand angemeldet ist** – Fragen Sie den Benutzer, ob es in Ordnung ist, eine Fernsteuerungssitzung zu beginnen. Der Text dieser Frage kann im Bearbeitungsfeld unterhalb dieser Option bearbeitet werden. Die Fernsteuerung kann erst beginnen, wenn der Benutzer auf die Schaltfläche **Ja** klickt. Wenn nach einer Minute keine Option angeklickt wurde, wird **Nein** angenommen und VSA entfernt das Dialogfeld vom Zielrechner. Die Fernsteuerungssitzung wird abgebrochen.

- **Benutzer benachrichtigen, wenn die Sitzung beendet ist** – Benachrichtigt den Benutzer, wenn die Fernsteuerungssitzung beendet wird.
- **Administratormitteilung für Start von Remote Control erforderlich** – Aktivieren Sie dieses Kontrollkästchen, damit VSA-Benutzer vor dem Start der Fernsteuerungssitzung eine Anmerkung eingeben müssen. Die Anmerkung ist im Fernsteuerungsprotokoll enthalten und wird dem Rechnerbenutzer nicht angezeigt.

Richtlinien – Registerkarte "Einstellungen – Zuweisung Softwarebereitstellungsprofil

Policy Management > Richtlinien > Registerkarte ''Einstellungen > Kontrollkästchen ''Zuweisung Softwarebereitstellungsprofil''

Die Kategorie **Zuweisung Softwarebereitstellungsprofil** weist einer Richtlinie ein **Software Deployment and Update**-Profil und ein Zeitplanmuster zu. Auf Rechnern, denen diese Richtlinie zugewiesen ist, muss **Software Deployment and Update** installiert sein.

- **Bereitstellungs-Muster** – Der Zeitplan für die periodische Bereitstellung. Zeitplanmuster werden mit der Registerkarte Software Deployment and Update > **Anwendungseinstellungen** *(http://help.kaseya.com/webhelp/DE/KSDU/9000000/index.asp#9819.htm)* > **Zeitplanmuster** konfiguriert.
- **Profil hinzufügen** – Fügt ein **Software Deployment and Update Profil** *(http://help.kaseya.com/webhelp/DE/KSDU/9000000/index.asp#9815.htm)* zu dieser Richtlinie hinzu.
- **Profil entfernen** – Entfernt ein Profil aus dieser Richtlinie.

Richtlinien – Registerkarte "Einstellungen" – Neustart für Softwarebereitstellung

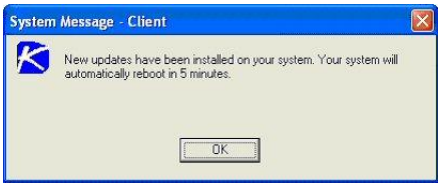
Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Neustart für Softwarebereitstellung''

Die Richtlinienkategorie **Neustart für Softwarebereitstellung** weist einer Richtlinie eine **Software**

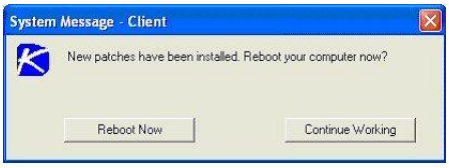
Deployment and Update-Neustartaktion

(http://help.kaseya.com/webhelp/DE/KSDU/9000000/index.asp#9821.htm) zu. Auf Rechnern, denen diese Richtlinie zugewiesen ist, muss **Software Deployment and Update** installiert sein.

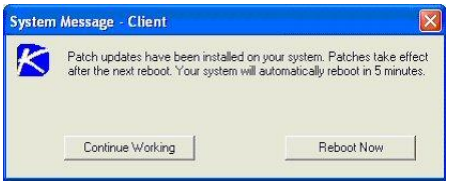
- **Neustart sofort nach Update** – Startet den Computer sofort nach Abschluss der Installation neu.
- **Neustart am <Wochentag> um <Uhrzeit> nach Installation** – Nach Abschluss der Patch-Installation wird der Computer am ausgewählten Tag zur ausgewählten Uhrzeit neu gestartet. Anhand dieser Einstellungen können Sie Patches tagsüber installieren, wenn Benutzer angemeldet sind, und dann nachts einen Neustart erzwingen. Wenn **jeden Tag** ausgewählt ist, wird der Rechner zum angegebenen Zeitpunkt nach Abschluss der Patch-Installation neu gestartet.
- **Benutzer warnen, dass der Rechner in <N> Minuten neu startet (ohne Anfrage auf Genehmigung)** – Wenn eine Patch-Installation abgeschlossen ist, wird die nachstehende Meldung angezeigt, die den Benutzer warnt und ihm die angegebene Anzahl von Minuten anzeigt, um seinen aktuellen Arbeitsschritt abzuschließen und seine Arbeit zu speichern. Falls niemand angemeldet ist, startet das System sofort neu.


System Message - Client
New updates have been installed on your system. Your system will automatically reboot in 5 minutes.
OK

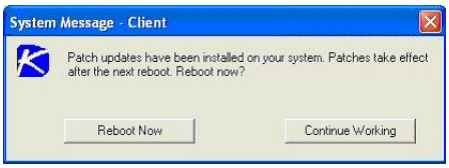
- **Neustart übergehen, falls Benutzer angemeldet ist** – Wenn der Benutzer angemeldet ist, wird der Neustart nach Abschluss der Patch-Installation übergangen. Verwenden Sie diese Einstellung, um eine Störung der Benutzer zu vermeiden. Dies ist die Standardeinstellung.
- **Falls der Benutzer angemeldet ist, Neustart anfragen alle <N> Minuten bis zum Neustart** – Bei dieser Einstellung wird die nachstehende Meldung angezeigt, in der der Benutzer gefragt wird, ob jetzt ein Neustart durchgeführt werden kann. Wenn sich niemand am Computer befindet oder der Benutzer mit 'Nein' antwortet, wird die gleiche Meldung alle N Minuten angezeigt, bis das System neu gestartet wird. Falls niemand angemeldet ist, startet das System sofort neu.



- **Um Erlaubnis fragen, falls der Benutzer angemeldet ist. Neu starten, wenn keine Antwort erfolgt nach <N> Minuten. Neustart, wenn der Benutzer nicht angemeldet ist** – Bei dieser Einstellung wird die nachstehende Meldung angezeigt, in der der Benutzer gefragt wird, ob jetzt ein Neustart durchgeführt werden kann. Falls sich niemand am Computer befindet, wird dieser automatisch nach N Minuten gestartet, **ohne dass offene Dokumente gespeichert werden**. Falls niemand angemeldet ist, startet das System sofort neu.


System Message - Client
Patch updates have been installed on your system. Patches take effect after the next reboot. Your system will automatically reboot in 5 minutes.
Continue Working
Reboot Now

- **Um Erlaubnis fragen, falls der Benutzer angemeldet ist. Keine Aktion, wenn keine Antwort erfolgt nach <N> Minuten. Neustart, wenn der Benutzer nicht angemeldet ist** – Bei dieser Einstellung wird die nachstehende Meldung angezeigt, in der der Benutzer gefragt wird, ob jetzt ein Neustart durchgeführt werden kann. Wenn sich niemand am Computer befindet, wird der Neustart übergangen. Falls niemand angemeldet ist, erfolgt sofort ein Neustart.


System Message - Client
Patch updates have been installed on your system. Patches take effect after the next reboot. Reboot now?
Reboot Now
Continue Working

- **Nicht neu starten nach Aktualisierung** – Startet nicht neu. Diese Einstellung wird in der Regel für Server verwendet, bei denen der Neustart kontrolliert durchgeführt werden muss. Sie können per E-Mail benachrichtigt werden, wenn ein neuer Patch installiert wurde, Hierfür aktivieren Sie **E-Mail senden, wenn Neustart erforderlich** und geben eine E-Mail-Adresse ein.

Richtlinien – Registerkarte "Einstellungen" – Zuweisung Softwarebereitstellungsscan

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Zuweisung Softwarebereitstellungsscan''

Die Kategorie **Scan-Zeitplan für Softwarebereitstellung** weist einer Richtlinie einen **Software Deployment and Update** Scan-Zeitplan zu. Auf Rechnern, denen diese Richtlinie zugewiesen ist, muss **Software Deployment and Update** installiert sein. Zeitplanmuster werden mit der Registerkarte Software Deployment and Update > **Anwendungseinstellungen** *(http://help.kaseya.com/webhelp/DE/KSDU/9000000/index.asp#9819.htm)* > **Zeitplanmuster** konfiguriert.

- **Referenzscan** – Der Zeitplan für den periodischen Referenzscan.
- **Letzter Scan** – Der letzte periodische Scan-Zeitplan.

Richtlinien – Registerkarte "Einstellungen" – Alarme unterbrechen

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Alarme unterbrechen''

Die Kategorie **Alarme unterbrechen** weist einer Richtlinie einen Zeitplan zum **Alarm unterbrechen** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#2185.htm)* zu. Wenn Alarme für eine Rechner-ID ausgesetzt sind, *sammelt der Agent weiterhin Daten, generiert jedoch keine zugehörigen Alarme*.

- **Zeitplan für Unterbrechen hinzufügen** – Konfiguriert Unterbrechungsalarme einmal oder für eine periodische Dauer.
  - **Alarme unterbrechen am <Datum> um <Uhrzeit>** – Gibt Startdatum und Startzeit an.
  - **Alle <N> Perioden wiederkehrend** – Geben Sie 0 ein oder lassen Sie dieses Feld leer, um Alarme nur einmal zu unterbrechen.
  - **Alarme unterbrechen für <N> Perioden** – Stellen Sie die Dauer ein, für die Alarme unterbrochen werden.
- **Unterbrechungszeitplan entfernen**

Richtlinien – Registerkarte "Einstellungen" – Liste nach Scan aktualisieren

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Liste nach Scan aktualisieren''

Die Kategorie **Liste nach Scan aktualisieren** weist einer Richtlinie Zeitpläne für **Liste nach Scan aktualisieren** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#1948.htm)* zu.

Für Windows 2000 und ältere Windows-Rechner – Benutzer können wählen, die Option **Listen durch Scan aktualisieren** immer wieder periodisch auszuführen, um neue Zählerobjekte auf diesen Rechnern zu ermitteln. Dies ist der einzige Grund, um **Listen durch Scan aktualisieren** periodisch auszuführen.

- **Planung bearbeiten** – Bearbeitet einen vorhandenen Scan-Zeitplan. Planen Sie die einmalige oder periodische Ausführung einer Aufgabe. Bei jeder Art der Wiederholung (einmal, minütlich, stündlich, täglich, wöchentlich, monatlich) werden weitere verfügbare Optionen angezeigt. Periodische Zeitplanung bedeutet, dass Sie Start- und Endtermine für die Wiederholung einstellen müssen. Mögliche Optionen:
  - **Der Zeitplan wird auf der Zeitzone des Agent basieren (statt der des Servers).** – Wenn diese Option ausgewählt wird, legen die Zeiteinstellungen im Dialogfeld "Scheduler" anhand der lokalen Zeit des Agent-Rechners fest, wann die Aufgabe ausgeführt werden soll. Andernfalls beziehen sich die Zeitangeben auf die Serverzeit, die unter "System > Einstellungen" festgelegt ist. Übernimmt die Standardeinstellungen aus der Seite "System > Standardeinstellungen".
  - **Verteilungsfenster** – Plant die Aufgabe zu einem willkürlichen Zeitpunkt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen. Beispiel: Wenn die Ausführung einer Aufgabe für 3:00 Uhr geplant ist und das Verteilungsfenster 1 Stunde beträgt, wird die Zeitplanung für die Aufgabe in einen zufälligen Zeitpunkt zwischen 3:00 und 4:00 Uhr geändert.
  - **Überspringen, wenn offline** – Falls dies aktiviert und der Rechner offline ist, wird dies übergangen und zur nächsten geplanten Uhrzeit ausgeführt. Wenn diese Option leer gelassen wird und der Rechner offline ist, führen Sie die Aufgabe aus, sobald der Rechner wieder online ist.
  - **Bei offline einschalten** – Nur Windows. Wenn dies aktiviert ist, wird der Rechner hochgefahren, falls er offline ist. Erfordert Wake-On-LAN oder vPro und ein anderes verwaltetes System auf dem gleichen LAN.
  - **Folgenden Zeitrahmen ausschließen** – **Bezieht sich ausschließlich auf das Verteilungsfenster.** Falls markiert, wird ein Zeitrahmen im Verteilungsfenster angegeben, in dem die Aufgabe nicht geplant werden kann. Zeitangaben außerhalb des Verteilungsfensters werden ignoriert.
- **Zurücksetzen** – Für diesen Scantyp ist bei dieser Richtlinie kein Zeitplan eingestellt. Wenn für den gleichen Scantyp in einer Richtlinie mit niedrigerer Priorität ein Zeitplan definiert ist, so *darf* er wirksam werden.
- **Keine** – Für diesen Scantyp ist bei dieser Richtlinie kein Zeitplan eingestellt. Wenn für den gleichen Scantyp in einer Richtlinie mit niedrigerer Priorität ein Zeitplan definiert ist, so *darf er nicht* wirksam werden.

Richtlinien – Registerkarte "Einstellungen" – Arbeitsverzeichnis

Policy Management > Richtlinien > Registerkarte ''Einstellungen'' > Kontrollkästchen ''Arbeitsverzeichnis''

Die Kategorie **Arbeitsverzeichnis** weist einer Richtlinie ein **Arbeitsverzeichnis** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#368.htm)* zu.

- **Arbeitsverzeichnis** – Stellt den Pfad zu einem Verzeichnis auf dem verwalteten Rechner ein, der vom Agent zum Speichern der Arbeitsdateien verwendet wird.

Einstellungen

Policy Management > Einstellungen

Die Seite **Einstellungen** plant das Intervall für die automatische Bereitstellung aller Richtlinien auf allen zugewiesenen Rechnern.

Bereitstellungsintervall

Diese Einstellung bestimmt, wie oft Richtlinien implementiert werden. Richtlinien können mit Rechnern, Rechnergruppen oder Unternehmen verknüpft sein. Wenn neue Rechner auftreten oder ihre bestehenden Verknüpfungen geändert werden, müssen Richtlinien eventuell verteilt bzw. neu bereitgestellt werden. Durch Einstellen des Bereitstellungsintervall auf "manuell" muss der Benutzer die Schaltfläche **Jetzt anwenden** auf der Seite **Richtlinien** *(siehe 6)* anklicken, um eine Richtlinie bereitzustellen.

Hinweis: Policy Management verfügt über einen periodischen Prozess, der automatisch Änderungen der Ansichtsmitgliedschaft bei allen Agent-Rechnern erkennt. Dies ist ein sehr intensiver Prozess. Darum ist der Zeitplan für diesen Prozess nicht an das **Bereitstellungsintervall** gebunden. Stattdessen wird der Prozess zur Ansichtsmitgliedschaft einmal pro Stunde ausgeführt, anhand eines vom System eingestellten Zeitplans. Wenn Sie die Ansichtsmitgliedschaft sofort neu bewerten möchten, können Sie die Schaltfläche **Rechner** *(siehe 33)* > **Richtlinien erneut verarbeiten** für einen oder mehrere ausgewählte Rechner verwenden.

Planung bearbeiten

Eine Compliance-Kontrolle vergleicht die Agent-Einstellungen mit den Richtlinien, die diesem Agent zugewiesen sind, um festzustellen, ob diese eingehalten werden. Bei Richtlinien, für die Anmeldedaten eingestellt werden müssen, stellt **Policy Management** jetzt den Richtlinien-Objektstatus als "Erfüllt Richtlinien nicht mehr" ein, wenn die Richtlinie aufgrund eines nicht unterstützten Betriebssystems oder ungültigen Agent-Anmeldeinformationen nicht verarbeitet werden kann.

Klicken Sie auf **Planung bearbeiten**, um das Fenster **Plan-Compliance-Kontrolle** anzuzeigen. Jede Art der Wiederholung (einmal, minütlich, täglich, wöchentlich, monatlich, jährlich) zeigt weitere Optionen für diese Art der Wiederholung an. Periodische Zeitplanung bedeutet, dass Sie Start- und Endtermine für die Wiederholung einstellen müssen. *Nicht alle Optionen stehen für jede geplante Aufgabe zur Verfügung.* Optionen können Folgendes umfassen:

- **Der Zeitplan wird auf der Zeitzone des Agent basieren (statt der des Servers).** – Wenn diese Option ausgewählt wird, legen die Zeiteinstellungen im Dialogfeld "Scheduler" anhand der lokalen Zeit des Agent-Rechners fest, wann die Aufgabe ausgeführt werden soll. Andernfalls beziehen sich die Zeitangeben auf die Serverzeit, die unter "System > Einstellungen" festgelegt ist. Übernimmt die Standardeinstellungen aus der Seite "System > Standardeinstellungen".

- **Verteilungsfenster** – Plant die Aufgabe zu einem willkürlichen Zeitpunkt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen. Beispiel: Wenn die Ausführung einer Aufgabe für 3:00 Uhr geplant ist und das Verteilungsfenster 1 Stunde beträgt, wird die Zeitplanung für die Aufgabe in einen zufälligen Zeitpunkt zwischen 3:00 und 4:00 Uhr geändert.
- **Überspringen, wenn offline** – Falls dies aktiviert und der Rechner offline ist, wird dies übergangen und zur nächsten geplanten Uhrzeit ausgeführt. Wenn diese Option leer gelassen wird und der Rechner offline ist, führen Sie die Aufgabe aus, sobald der Rechner wieder online ist.
- **Bei offline einschalten** – Nur Windows. Wenn dies aktiviert ist, wird der Rechner hochgefahren, falls er offline ist. Erfordert Wake-On-LAN oder vPro und ein anderes verwaltetes System auf dem gleichen LAN.
- **Folgenden Zeitrahmen ausschließen** – **Bezieht sich ausschließlich auf das Verteilungsfenster.** Falls markiert, wird ein Zeitrahmen im Verteilungsfenster angegeben, in dem die Aufgabe nicht geplant werden kann. Zeitangaben außerhalb des Verteilungsfensters werden ignoriert.

Zurücksetzen

- Entfernt die geplante Compliance-Kontrolle.

Organisationen/Rechnergruppen

Policy Management > Unternehmen / Rechnergruppen

Die Seite **Unternehmen / Rechnergruppen** weist Richtlinien Unternehmen und Rechnergruppen zu. Ein **System-Cabinet** *(siehe 40)* bietet integrierte Richtlinien, die Best-Practice-Lösungen für gewöhnliche IT-Verwaltungsaufgaben darstellen. Richtlinien können mithilfe des **Systems Management Configuration Installationsassistenten** *(http://help.kaseya.com/webhelp/DE/SSP/9000000/index.asp#11220.htm)* und dieser System-Cabinet-Richtlinien automatisch für ein Unternehmen konfiguriert werden.

Aktionen

- **Entfernen** – Entfernt eine ausgewählte Richtlinie aus einem Unternehmen oder einer Rechnergruppe.
- **Auswählen & Zuweisen** – Wählt eine Richtlinie für ein Unternehmen oder eine Rechnergruppe aus und weist sie zu. Diese Schaltfläche wird nur aktiv, wenn der ausgewählten Richtlinie eine Ansicht zugewiesen ist und sowohl die Richtlinie als auch mindestens ein Unternehmen oder eine Rechnergruppe ausgewählt ist.
- **Alle markieren** – Wählt alle Unternehmen aus.
- **Auswahl aufheben für alle** – Hebt die Auswahl von allen Unternehmen auf.
- **Alle ausblenden** – Blendet die Unternehmens-/Rechnergruppenstruktur vollständig aus.
- **Alle ausweiten** – Erweitert die Unternehmens-/Rechnergruppenstruktur vollständig.
- **Erinnern, dass Elemente beim Verschieben automatisch synchronisiert werden** – Bei Markierung wird eine Pop-up-Warnung darüber angezeigt, dass Änderungen sofort angewendet werden. Gilt individuell für jeden VSA-Benutzer.
- **(Ordnerstrukturfilter)** – Gilt für das **Rechnergruppen**-Cabinet und das **Richtlinien**- und System-Cabinet – Geben Sie Text in das Bearbeitungsfeld des Filters ein und klicken Sie dann auf das Trichtersymbol , um die Ordnerstruktur zu filtern. Beim Filtern wird nicht zwischen Groß-/Kleinschreibung unterschieden. Eine Übereinstimmung trifft ein, wenn Filtertext irgendwo in der Ordnerstruktur gefunden wird.

Zuweisen von Richtlinien

Ziehen Sie eine Richtlinie aus der Ordnerstruktur **Richtlinien** im rechten Fensterbereich in die Ordnerstruktur **Rechnergruppen** im mittleren Fensterbereich.

Richtlinien ohne Ansichten

Auf der Seite Richtlinien *muss* einer Richtlinie eine Ansicht zugewiesen werden, um eine Richtlinie mit der Seite **Unternehmen/Rechnergruppen** *(siehe 30)* zuzuweisen. *So wird verhindert, dass eine Richtlinie unbeabsichtigt allen Rechner in VSA zugewiesen wird.* Eine Richtlinie ohne angegebene Ansicht wird mit einem roten Symbol zum Blättern in der Richtlinienstruktur auf der Seite **Unternehmen/Rechnergruppen** angezeigt und gibt so an, dass sie nicht zugewiesen werden kann. Ein Ordner mit einem roten Ausrufezeichen wird in der Richtlinienstruktur angezeigt, wenn diese mindestens eine Richtlinie ohne angegebene Ansicht enthält. Beim Zuweisen eines gesamten Richtlinienordners zu einem Unternehmen oder einer Rechnergruppe werden Richtlinien ohne angegebene Ansicht ignoriert.

Regeln zur Richtlinienzuweisung

- Jedem Unternehmen, jeder Rechnergruppe oder jedem Rechner können mehrere Richtlinien zugewiesen werden.
- Bei einem Rechner mit mehreren zugewiesenen Richtlinien kommt es zu **in Konflikt miteinander stehenden Richtlinien**, wenn diese den *gleichen* Richtlinientyp angeben.
  - Mehrere Richtlinien stehen nicht in Konflikt miteinander, wenn unterschiedliche Richtlinientypen angegeben werden.
  - Die folgenden Richtlinientypen sind **miteinander kombinierbar**, sodass keine Konflikte auftreten.
    - ✓ Ereignisprotokoll-Benachrichtigungen, Dateien verteilen, Monitor-Sets und Agent-Verfahren.
- Richtlinien werden *nach Unternehmen/Rechnergruppe* über die Seite **Unternehmen/Rechnergruppen** *(siehe 31)* zugewiesen.
  - Richtlinien, die innerhalb der Unternehmenshierarchie einer niedrigeren Stufe zugewiesen sind, haben Vorrang vor Richtlinien, die einer höheren Stufe in derselben Unternehmenshierarchie zugewiesen sind.
  - Richtlinien, die einer Stufe zugewiesen sind, gelten für alle niedrigeren Stufen, es sei denn, sie stehen in Konflikt mit einer Richtlinie auf einer niedrigeren Stufe.
  - Wenn einem Unternehmen oder einer Rechnergruppe mehrere Richtlinien zugewiesen sind, haben die Richtlinien Vorrang, die in der Reihenfolge oben stehen.
- Richtlinien können *nach Rechner* mit der Seite **Rechner** *(siehe 33)* zugewiesen werden.
  - Richtlinien, die *nach Rechner* zugewiesen sind, haben Vorrang vor allen Richtlinien, die diesem Rechner *nach Unternehmen/Rechnergruppe* zugewiesen sind.
  - Die Rangordnung von Richtlinien, die nach Rechner zugewiesen sind, entspricht der angegebenen Reihenfolge.
- Alle Richtlinienzuweisungen können *überschrieben* werden, indem die Agent-Einstellungen *manuell* im gesamten VSA geändert werden.
  - Manuelle Änderungen haben Vorrang vor allen anderen Richtlinienzuweisungen.
- Eine Richtlinie kann mit einer *Ansichtsdefinition* auf der Seite **Richtlinien** *(siehe 6)* verknüpft sein.
  - Wenn ein Rechner einer Richtlinie *nach Unternehmen* oder *nach Rechnergruppe* zugewiesen ist, *filtert* eine verknüpfte Ansicht die mit einer Richtlinie verknüpften Rechner. Wenn ein Rechner nicht Mitglied der Ansichtsdefinition ist, so wird die Richtlinie nicht auf diesen Rechner übertragen.
  - Wenn ein Rechner einer Richtlinie *nach Rechner* zugewiesen ist, so wird die mit einer Richtlinie verknüpfte Ansicht ignoriert und die Richtlinie wird auf den Rechner übertragen.
  - Das Verknüpfen einer Richtlinie mit einer Ansicht weist die Richtlinie *nicht von selbst* einem Rechner zu.
- Die Rangordnung von Ansichten hängt von den Richtlinien ab, mit denen sie verknüpft sind.

Rechner

Policy Management > Rechner

Die Seite **Rechner** weist Richtlinien einzelnen Rechnern zu. Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope.

Rechner-Konformitätsstatus

Das Feld in der Mitte zeigt den Richtlinien-Konformitätsstatus für jeden Rechner in der folgenden Rangordnung an.

– `Erfüllt Richtlinien` – Die Agent-Einstellungen für diesen Rechner entsprechen den Einstellungen aller diesem Rechner zugeordneten Richtlinien.

– `Erfüllt Richtlinien nicht mehr` – Mindestens eine Agent-Einstellung entspricht mindestens einer aktiven Richtlinie, die diesem Rechner zugewiesen ist, nicht.

– `Zur Bereitstellung gekennzeichnet`– Es wurde mindestens eine diesem Rechner zugewiesene Richtlinie geändert und deren Bereitstellung geplant.

– `Überschrieben` – Mindestens eine Agent-Einstellung entspricht mindestens einer aktiven Richtlinie, die diesem Rechner zugewiesen ist, *aufgrund einer Benutzerüberschreibung* nicht. Eine Überschreibung tritt auf, wenn eine Agent-Einstellung manuell von einem VSA-Benutzer an einem beliebigen Ort im System vorgenommen wird. Wenn auch nur eine einzelne Agent-Einstellung in einer einem Rechner zugewiesenen Richtlinie überschrieben wird, werden keine weiteren Agent-Einstellungen in dieser Richtlinie auf diesem Rechner durchgesetzt. Andere demselben Rechner zugewiesenen Richtlinien behalten ihre Gültigkeit.

Hinweis: Klicken Sie auf das Symbol Richtlinienstatus, um das Fenster **Richtlinienmatrix** *(siehe 4)* > **Matrix-Details** für den jeweiligen Rechner anzuzeigen.

Aktionen

- **Zuweisen** – Weist Richtlinien ausgewählten Rechnern zu.
- **Überschreiben aufheben** – Löscht **Policy Management**-Richtlinienüberschreibungen auf ausgewählten Rechnern. *Nach Klicken auf* **Überschreiben aufheben** *muss der Benutzer auf* **Richtlinien erneut verarbeiten** *klicken, um sicherzustellen, dass die ehemals überschriebenen Richtlinienobjekte erneut auf den Agent angewendet werden.* Die Bedingung einer **Policy Management**-Richtlinienüberschreibung besteht, wenn Agent-Einstellungen für einen Rechner außerhalb des **Policy Management**-Moduls manuell eingestellt wurden. Werden zum Beispiel Änderungen am Agent-Menü eines Rechners über die Seite **Agent-Menü** im **Agent**-Modul vorgenommen, so wird eine Überschreibbedingung für diesen Agent-Rechner erstellt. **Policy Management**Richtlinien werden von da an ignoriert. Durch Löschen einer Überschreibung können angewendete **Policy Management**-Richtlinien gültig werden.
- **Richtlinien erneut verarbeiten** – Alle einem Rechner zugewiesenen Richtlinienobjekte können zur Bereitstellung erneut markiert und verarbeitet werden, so als ob sie diesem Rechner zum ersten Mal zugewiesen würden. Um unnötige Serveraktivität und Netzwerkdatenverkehr zu reduzieren, wird jedes Richtlinienobjekt nur *einmal* auf einem Rechner bereitgestellt, selbst wenn dem Rechner zusätzliche Richtlinien zugewiesen werden, in denen dasselbe Richtlinienobjekt enthalten ist. Verwenden Sie diese Option zur erneuten Bereitstellung aller Richtlinienobjekte, die einem Rechner zugewiesen sind, wenn Agent-Einstellungen für einen Rechner unerwartet sind.

Rechter Fensterbereich

Der rechte Fensterbereich ist in zwei horizontale Abschnitte unterteilt.

- **Diesem Rechner zugeordnete Richtlinien** – Zeigt zugewiesene Richtlinien nach Rechner geordnet an.
- **Diesem Rechner zugeordnete Richtlinien in Verbindung mit Organisationen/Rechnergruppen** – Zeigt zugewiesene Richtlinien nach Organisation und Rechnergruppe geordnet an.

Aktionen

- **Nach oben verschieben** und **Nach unten verschieben** – Sie können die Reihenfolge der dem Rechner zugewiesenen Richtlinien neu ordnen.
- **Entfernen** – Sie können die dem Rechner zugewiesenen Richtlinien entfernen.

Regeln zur Richtlinienzuweisung

- Jedem Unternehmen, jeder Rechnergruppe oder jedem Rechner können mehrere Richtlinien zugewiesen werden.
- Bei einem Rechner mit mehreren zugewiesenen Richtlinien kommt es zu **in Konflikt miteinander stehenden Richtlinien**, wenn diese den *gleichen* Richtlinientyp angeben.
  - Mehrere Richtlinien stehen nicht in Konflikt miteinander, wenn unterschiedliche Richtlinientypen angegeben werden.
  - Die folgenden Richtlinientypen sind **miteinander kombinierbar**, sodass keine Konflikte auftreten.
    - ✓ Ereignisprotokoll-Benachrichtigungen, Dateien verteilen, Monitor-Sets und Agent-Verfahren.
- Richtlinien werden *nach Unternehmen/Rechnergruppe* über die Seite **Unternehmen/Rechnergruppen** *(siehe 31)* zugewiesen.
  - Richtlinien, die innerhalb der Unternehmenshierarchie einer niedrigeren Stufe zugewiesen sind, haben Vorrang vor Richtlinien, die einer höheren Stufe in derselben Unternehmenshierarchie zugewiesen sind.
  - Richtlinien, die einer Stufe zugewiesen sind, gelten für alle niedrigeren Stufen, es sei denn, sie stehen in Konflikt mit einer Richtlinie auf einer niedrigeren Stufe.
  - Wenn einem Unternehmen oder einer Rechnergruppe mehrere Richtlinien zugewiesen sind, haben die Richtlinien Vorrang, die in der Reihenfolge oben stehen.
- Richtlinien können *nach Rechner* mit der Seite **Rechner** *(siehe 33)* zugewiesen werden.
  - Richtlinien, die *nach Rechner* zugewiesen sind, haben Vorrang vor allen Richtlinien, die diesem Rechner *nach Unternehmen/Rechnergruppe* zugewiesen sind.
  - Die Rangordnung von Richtlinien, die nach Rechner zugewiesen sind, entspricht der angegebenen Reihenfolge.
- Alle Richtlinienzuweisungen können *überschrieben* werden, indem die Agent-Einstellungen *manuell* im gesamten VSA geändert werden.
  - Manuelle Änderungen haben Vorrang vor allen anderen Richtlinienzuweisungen.
- Eine Richtlinie kann mit einer *Ansichtsdefinition* auf der Seite **Richtlinien** *(siehe 6)* verknüpft sein.
  - Wenn ein Rechner einer Richtlinie *nach Unternehmen* oder *nach Rechnergruppe* zugewiesen ist, *filtert* eine verknüpfte Ansicht die mit einer Richtlinie verknüpften Rechner. Wenn ein Rechner nicht Mitglied der Ansichtsdefinition ist, so wird die Richtlinie nicht auf diesen Rechner übertragen.
  - Wenn ein Rechner einer Richtlinie *nach Rechner* zugewiesen ist, so wird die mit einer Richtlinie verknüpfte Ansicht ignoriert und die Richtlinie wird auf den Rechner übertragen.
  - Das Verknüpfen einer Richtlinie mit einer Ansicht weist die Richtlinie *nicht von selbst* einem Rechner zu.
  - Die Rangordnung von Ansichten hängt von den Richtlinien ab, mit denen sie verknüpft sind.

Policy Management – Agent-Richtlinienstatus

Info Center > Reporting > Berichte > Policy Management – Agent-Richtlinienstatus

- Wird nur angezeigt, wenn das Policy Management-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Agent-Richtlinienstatus** wird ein Richtlinienstatusbericht generiert. Dies kann nach Folgendem gefiltert werden:

- **Agent-Richtlinienstatus**
- **Richtlinien-Objekttyp**
- **Richtlinien-Objektstatus**

Policy Management – Richtliniendaten & Zuordnung

Info Center > Reporting > Berichte > Policy Management – Richtliniendaten & Zuordnung

- Wird nur angezeigt, wenn das Policy Management-Zusatzmodul installiert ist.

Mit der Berichtsdefinition **Richtliniendaten & Zuordnung** wird ein Bericht zu Richtliniendaten und Zuordnungen generiert. Dies kann nach Folgendem gefiltert werden:

- **Richtlinienstatus**
- **Richtlinien-Objekttyp**

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

©2015 Kaseya. All rights reserved. | www.kaseya.com

Glossar

Anmeldedaten

Als Anmeldedaten bezeichnet man den Benutzernamen und das Kennwort, die zur Authentifizierung des Zugriffs auf einen Rechner, ein Netzwerk oder eine andere Ressource durch einen Benutzer oder einen Prozess verwendet werden.

Agent-Anmeldeinformationen

Legen Sie über die Seite Agent > Anmeldedaten eingeben einen *einzelnen Satz* von Anmeldeinformationen mit Administratorrechten zur Verwendungen durch einen Agent fest.

Verwaltete Anmeldeinformationen

Geben Sie *zusätzliche* Anmeldedaten auf drei verschiedenen Ebenen an: nach Organisation, nach Rechnergruppe und nach einzelnem Rechner oder Gerät. Sie werden mithilfe von drei Navigationselementen im Modul **Audit** verwaltet:

- Bestand anzeigen – Erstellen Sie über diese Seite mehrere Sätze von Anmeldeinformationen für *einzelne* Rechner oder Geräte.
- Anmeldeinformationen verwalten – Erstellen Sie über diese Seite mehrere Sätze von Anmeldeinformationen für *Unternehmen* und *Rechnergruppen* innerhalb von Unternehmen.
- Anmeldeinformationen-Protokoll – Auf dieser Seite werden die Erstellung, die Anzeige und die Löschung verwalteter Anmeldeinformationen protokolliert.

Verwenden Sie verwaltete Anmeldeinformationen nach ihrer Erstellung zu Folgendem:

- Für die sofortige Suche aller Anmeldeinformationen, die für den Rechner, an dem Sie gerade arbeiten, gelten. Das Popup-Fenster **Schnellanzeige** enthält jetzt die Option **Anmeldeinformationen anzeigen**. Zugriff wird nach Rolle und Bereich gesteuert. Sie können jedem Satz von Anmeldeinformationen eine Beschreibung hinzufügen.
- Als Quell-Anmeldeinformationen für Agent-Anmeldeinformationen in einer Richtlinie. Aktivieren Sie in den Einstellungen **Anmeldedaten** auf der Seite Policy Management > Richtlinien das Kontrollkästchen **Standardeinstellungen von Unternehmen verwenden**, um die Verknüpfung einzurichten.

> **Hinweis:** Die Einstellungen unter Agent > Anmeldedaten eingeben können nicht direkt durch verwaltete Anmeldeinformationen überschrieben werden. Verwaltete Anmeldeinformationen müssen auf eine Richtlinie angewendet und diese Richtlinie muss wiederum auf einen Rechner angewendet werden.

Wenn für einen Rechner mehrere Sätze von Anmeldeinformationen definiert sind, hat die lokal am nächsten liegende Ebene Vorrang: nach Einzelrechner, nach Rechnergruppe oder nach Unternehmen. Auf jeder dieser Ebenen kann nur jeweils ein Satz verwalteter Anmeldeinformationen als Quell-Anmeldeinformationen für die Agent-Anmeldeinformationen designiert werden.

Lokal

Eine **lokale** Hardware-/Softwareinstallation des VSA wird von einem Dienstanbieter gepflegt und in der Regel nur von diesem Dienstanbieter eingesetzt. Siehe **Software as a Service (SaaS)** *(siehe 40)*.

myOrg

`myOrg` ist die **Organisation** *(siehe 38)* des Dienstanbieters, der den VSA verwendet. Alle anderen Organisationen im VSA sind Fremdorganisationen, die mit `myOrg` geschäftliche Beziehungen unterhalten. Der Standardname `myOrg`, `My Organization`, sollte in den Firmennamen des Dienstanbieters umbenannt werden. *Dieser Name wird oben auf verschiedenen Berichten angezeigt,*

um dem Bericht ein Branding zu verleihen. Agents, die auf intern verwalteten Rechnern installiert sind, können dieser Organisation zugewiesen werden. *VSA-Benutzeranmeldedaten sind üblicherweise mit Mitarbeiterdatensätzen in der Organisation* `myOrg` *verknüpft.* `myOrg` kann keiner übergeordneten Organisation zugeordnet werden.

Org

Der VSA unterstützt drei verschiedene Arten von Geschäftsbeziehungen:

- **Unternehmen** – Unterstützung von Rechnergruppen und Verwaltung von Rechnern mittels Agents.
- **Kunden** – Unterstützung der Fakturierung von Kunden mittels **Service Billing**.
- **Anbieter** – Unterstützung der Materialbeschaffung mittels **Service Billing**.

Die `Org`-Tabelle ist eine Supporttabelle, die von *Unternehmen*, *Kunden* und *Anbietern* gemeinsam genutzt wird. Jeder Datensatz in der `Org`-Tabelle wird durch eine eindeutige `orgID` identifiziert. Die `Org`-Tabelle enthält grundlegende Informationen, die Sie generell zur Pflege von Geschäftsbeziehung aller Art benötigen: Postanschrift, primäre Telefonnummer, DUNS-Nummer, Jahreseinnahmen usw. Da die `Org`-Tabelle gemeinsam genutzt wird, können Sie folgende Umwandlungen mühelos vornehmen:

- Einen Kunden in ein Unternehmen oder einen Anbieter
- Einen Anbieter in ein Unternehmen oder einen Kunden
- Ein Unternehmen in einen Kunden oder Anbieter

Hinweis: `myOrg` (siehe 37) ist die Organisation des Dienstanbieters, der den VSA verwendet.

Patch-Richtlinie

Patch-Richtlinien enthalten alle aktiven Patches zum Zweck des Bestätigens oder Ablehnens von Patches. Ein aktives Patch ist als ein Patch definiert, das durch einen Patch-Scan von mindestens einem Rechner im VSA gemeldet wurde. Ein Rechner kann als Mitglied einer oder mehrerer Patch-Richtlinie(n) festgelegt werden.

Sie können beispielsweise eine Patch-Richtlinie namens `servers` erstellen und alle Ihre Server als Mitglieder dieser Patch-Richtlinie zuweisen. Dann erstellen Sie eine weitere Patch-Richtlinie namens `workstations` und weisen alle Ihre Workstations als Mitglieder dieser Richtlinie zu. Auf diese Weise können Sie unterschiedliche Patch-Bestätigungen für Server und Workstations konfigurieren.

- Die Patches von Rechnern, die keine Mitglieder irgendeiner Patch-Richtlinie sind, werden als *automatisch bestätigt* angesehen.
- Beim Erstellen einer neuen Patch-Richtlinie wird ihr Standard-Bestätigungsstatus für alle Patch-Kategorien auf *Bestätigung ausstehend* gesetzt.
- Der Standard-Bestätigungsstatus für jede Kategorie von Patches und für jedes Produkt kann separat festgelegt werden.
- Falls ein Rechner ein Mitglied mehrerer Patch-Richtlinien ist und diese Richtlinien miteinander in Konflikt stehende Bestätigungsstatus aufweisen, so gilt der am meisten einschränkende Bestätigungsstatus.
- Für die Eingangsaktualisierung und Automatische Aktualisierung müssen Patches bestätigt werden, bevor sie installiert werden.
- Mit Bestätigung nach Richtlinie wird ein Patch nach *Richtlinie* bestätigt oder abgelehnt.
- Mit Bestätigung nach Patch werden Patches nach *Patch* bestätigt oder abgelehnt und der Bestätigungsstatus für dieses Patch in allen Patch-Richtlinien festgelegt.
- Mit KB überschreiben wird der Standard-Bestätigungsstatus nach *KB-Artikel* für alle Patch-Richtlinien überschrieben und der Bestätigungsstatus für diejenigen Patches, auf die sich der KB-Artikel bezieht, in allen Patch-Richtlinien festgelegt.
- Mit Patch-Aktualisierung und Rechneraktualisierung können auch abgelehnte Patches installiert werden.

- Benutzer, die keine Haupt- bzw. `Master`-Rolle innehaben, sehen nur die von ihnen selbst erstellten Patch-Richtlinien bzw. Patch-Richtlinien mit Rechner-IDs, deren Umfang den Benutzer zur Anzeige autorisieren.

Regeln zur Richtlinienzuweisung

- Jedem Unternehmen, jeder Rechnergruppe oder jedem Rechner können mehrere Richtlinien zugewiesen werden.
- Bei einem Rechner mit mehreren zugewiesenen Richtlinien kommt es zu **in Konflikt miteinander stehenden Richtlinien**, wenn diese den *gleichen* Richtlinientyp angeben.
  - Mehrere Richtlinien stehen nicht in Konflikt miteinander, wenn unterschiedliche Richtlinientypen angegeben werden.
  - Die folgenden Richtlinientypen sind **miteinander kombinierbar**, sodass keine Konflikte auftreten.
    - ✓ Ereignisprotokoll-Benachrichtigungen, Dateien verteilen, Monitor-Sets und Agent-Verfahren.
- Richtlinien werden *nach Unternehmen/Rechnergruppe* über die Seite **Unternehmen/Rechnergruppen** *(siehe 31)* zugewiesen.
  - Richtlinien, die innerhalb der Unternehmenshierarchie einer niedrigeren Stufe zugewiesen sind, haben Vorrang vor Richtlinien, die einer höheren Stufe in derselben Unternehmenshierarchie zugewiesen sind.
  - Richtlinien, die einer Stufe zugewiesen sind, gelten für alle niedrigeren Stufen, es sei denn, sie stehen in Konflikt mit einer Richtlinie auf einer niedrigeren Stufe.
  - Wenn einem Unternehmen oder einer Rechnergruppe mehrere Richtlinien zugewiesen sind, haben die Richtlinien Vorrang, die in der Reihenfolge oben stehen.
- Richtlinien können *nach Rechner* mit der Seite **Rechner** *(siehe 33)* zugewiesen werden.
  - Richtlinien, die *nach Rechner* zugewiesen sind, haben Vorrang vor allen Richtlinien, die diesem Rechner *nach Unternehmen/Rechnergruppe* zugewiesen sind.
  - Die Rangordnung von Richtlinien, die nach Rechner zugewiesen sind, entspricht der angegebenen Reihenfolge.
- Alle Richtlinienzuweisungen können *überschrieben* werden, indem die Agent-Einstellungen *manuell* im gesamten VSA geändert werden.
  - Manuelle Änderungen haben Vorrang vor allen anderen Richtlinienzuweisungen.
- Eine Richtlinie kann mit einer *Ansichtsdefinition* auf der Seite **Richtlinien** *(siehe 6)* verknüpft sein.
  - Wenn ein Rechner einer Richtlinie *nach Unternehmen* oder *nach Rechnergruppe* zugewiesen ist, *filtert* eine verknüpfte Ansicht die mit einer Richtlinie verknüpften Rechner. Wenn ein Rechner nicht Mitglied der Ansichtsdefinition ist, so wird die Richtlinie nicht auf diesen Rechner übertragen.
  - Wenn ein Rechner einer Richtlinie *nach Rechner* zugewiesen ist, so wird die mit einer Richtlinie verknüpfte Ansicht ignoriert und die Richtlinie wird auf den Rechner übertragen.
  - Das Verknüpfen einer Richtlinie mit einer Ansicht weist die Richtlinie *nicht von selbst* einem Rechner zu.
  - Die Rangordnung von Ansichten hängt von den Richtlinien ab, mit denen sie verknüpft sind.

Richtlinien und Ansichten

Auf der Seite Richtlinien *muss* einer Richtlinie eine Ansicht zugewiesen werden, um eine Richtlinie mit der Seite **Unternehmen/Rechnergruppen** *(siehe 30)* zuzuweisen. *So wird verhindert, dass eine Richtlinie unbeabsichtigt allen Rechner in VSA zugewiesen wird.* Eine Richtlinie ohne angegebene Ansicht wird mit einem roten Symbol zum Blättern in der Richtlinienstruktur auf der Seite **Unternehmen/Rechnergruppen** angezeigt und gibt so an, dass sie nicht zugewiesen werden kann. Ein Ordner mit einem roten Ausrufezeichen wird in der Richtlinienstruktur angezeigt, wenn diese mindestens eine Richtlinie ohne angegebene Ansicht enthält. Beim Zuweisen eines gesamten

Richtlinienordners zu einem Unternehmen oder einer Rechnergruppe werden Richtlinien ohne angegebene Ansicht ignoriert.

Richtlinienstatussymbol

- `In Compliance` – Die Agent-Einstellungen für diesen Rechner entsprechen den Einstellungen aller diesem Rechner zugewiesenen Richtlinien. Keine Benutzeraktion ist erforderlich.

- `Marked for Deployment` – Es wurde mindestens eine diesem Rechner zugewiesene Richtlinie geändert und so geplant, dass sie bereitgestellt wird. Keine Benutzeraktion ist erforderlich.

- `No Policy Attached` – Diesem Rechner sind keine *angewendeten* Richtlinien zugewiesen. Erwägen Sie, diesem Rechner *angewendete* Richtlinien zuzuweisen.

- `Out of Compliance` – Mindestens eine Agent-Einstellung entspricht nicht mindestens einer aktiven Richtlinie, die diesem Rechner zugewiesen ist. Ermitteln Sie mithilfe des Fensters **Richtliniendetails** die bestimmten Richtlinien und Einstellungen, die diese Nichtübereinstimmung verursachen.

- `Overridden` – Mindestens eine Agent-Einstellung entspricht nicht mindestens einer aktiven Richtlinie, die diesem Rechner zugewiesen ist, *aufgrund einer Benutzerüberschreibung*. Eine Überschreibung tritt auf, wenn eine Agent-Einstellung manuell von einem VSA-Benutzer an einem beliebigen Ort im System vorgenommen wird. Bestätigen Sie mithilfe des Fensters **Richtliniendetails**, dass das Überschreiben bestimmter Richtlinien und Einstellungen richtig ist. Wenn auch nur eine einzelne Agent-Einstellung in einer einem Rechner zugewiesenen Richtlinie überschrieben wird, werden keine weiteren Agent-Einstellungen in dieser Richtlinie auf diesem Rechner durchgesetzt. Andere demselben Rechner zugewiesenen Richtlinien behalten ihre Gültigkeit.

- `Inactive` – *Dieser Richtlinienstatus wird nur im Fenster* **Richtliniendetails** *angezeigt.* Wenn einem Rechner mehrere Richtlinien zugewiesen werden und sich die Agent-Einstellungen widersprechen, so wird durch **Regeln zur Richtlinienzuweisung** *(siehe 31)* festgelegt, welche Agent-Einstellungen befolgt und welche ignoriert werden. Ignorierte Einstellungen werden als inaktiv angezeigt. Als Rechnerstatus kann das Richtlinienstatussymbol `In Compliance` angezeigt werden, während im Fenster *Richtliniendetails* bestimmte Agent-Einstellungen in bestimmten Richtlinien als `Inactive` angezeigt werden. Dieses Verhalten wird erwartet. Keine Benutzeraktion ist erforderlich.

Richtlinienüberschreibungen

Die Bedingung einer **Policy Management**-Richtlinienüberschreibung besteht, wenn Agent-Einstellungen für einen Rechner außerhalb des **Policy Management**-Moduls manuell eingestellt wurden. Werden zum Beispiel Änderungen am Agent-Menü eines Rechners über die Seite **Agent-Menü** im **Agent**-Modul vorgenommen, so wird eine Überschreibbedingung für diesen Agent-Rechner erstellt. **Policy Management**Richtlinien werden von da an ignoriert. Durch Löschen einer Überschreibung können angewendete **Policy Management**-Richtlinien gültig werden.

Software as a Service (SaaS)

Kaseya bietet eine Software-as-a-Service (SaaS)-Bereitstellung von **Virtual System Administrator™** an. Dienstanbieter gehen eine vertragliche Beziehung mit Kaseya für den Zugriff auf einen von Kaseya gehosteten und gewarteten VSA ein und können eine bestimmte Anzahl ihrer Kunden-Agents installieren. Ihnen wird eine eindeutige *Tenant-Partition* eines gemeinsam genutzten Kaseya Server und einer Datenbank zugewiesen. Innerhalb ihrer zugewiesenen Partition können Dienstanbieter nur ihre eigenen Unternehmen, Rechnergruppen, Verfahren, Berichte und Tickets sehen. Die Dienstanbieter in einer Tenant-Partition haben vollen Zugriff auf alle Funktionen des VSA, mit Ausnahme der Systemwartung, die der Verantwortung von Kaseya unterliegt. Weitere Informationen finden Sie im Abschnitt **Lokal** *(siehe 37)*.

System-Cabinets

Integrierte Datenobjekte werden mit VSA und zusätzlichen Modulen bereitgestellt. Diese integrierten Datenobjekte, auch als *Inhalt* bezeichnet, bieten dem Benutzer Best-Practice-Lösungen für

gewöhnliche IT-Verwaltungsaufgaben. In manchen Fällen sind diese integrierten Datenobjekte nach *System-Cabinet* in einer Datenobjektstruktur organisiert. Dazu zählen:

- Richtlinien – Richtlinien-Verwaltung > Richtlinien
- Agent-Verfahren – Agent-Verfahren > Erstellen / Planen
- Monitor-Sets – Monitoring > Monitor-Sets

Integrierte Datenobjekte können nicht geändert werden, aber es kann eine Kopie erstellt werden, die Sie dann ändern können.

Token

Damit mehrere Unternehmen die gleichen integrierten Standardrichtlinien in **Policy Management** nutzen können, werden Platzhalter-**Token** in die Richtlinienfelder eingegeben; dazu ist eine E-Mail-Adresse erforderlich. Diese Token-Werte sind `#patchAlertEmail#`, `#sev1AlertEmail#`, `#sev2AlertEmail#` und `#sev3AlertEmail#`. VSA ersetzt automatisch ein Token in einer Richtlinie mit der entsprechenden E-Mail-Adresse des Unternehmens, wenn eine Alarmbenachrichtigung gesendet wird. Die E-Mail-Adressen der Unternehmen, auf die sich die Token beziehen, werden in Schritt 1 des **Assistenten zur Systemmanagement-Konfiguration** *(http://help.kaseya.com/webhelp/DE/SSP/9000000/index.asp#11221.htm)* angegeben. Dieser Assistent kann während der Einrichtung und jederzeit danach in der Registerkarte System > Orgn./Gruppen/Abtlg./Personal > Verwalten > **System-Management** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#11372.htm)* ausgeführt werden. Die **Policy Management**-Richtlinienkategorien, die E-Mail-Adressen enthalten, sind **Benachrichtigungen** *(siehe 10)*, **Monitor-Sets** *(siehe 18)* und **Patch-Einstellungen** *(siehe 23)*.

Inhaltsverzeichnis

A

Anmeldedaten • 37

B

Best Practices (System-Cabinets) • 40

D

Dashboard • 3

E

Einstellungen • 30

I

Inhalt (System-Cabinets) • 40

L

Lokal • 37

M

Machines • 33
myOrg • 37

O

Org • 38
Organisationen/Rechnergruppen • 31

P

Partition, • 40
Patch-Richtlinie • 38
Policies • 6
Policies - Settings tab • 8
Policy Management – Agent-Richtlinienstatus • 34
Policy Management – Richtliniendaten & Zuordnung • 35
Policy Management Modulvoraussetzungen • 3
Policy Management Überblick • 1
Protokolle • 4

R

Regeln zur Richtlinienzuweisung • 39
Richtlinien – Ordnerstruktur • 7
Richtlinien – Registerkarte "Einstellungen" – Agent-Menü • 9
Richtlinien – Registerkarte "Einstellungen" – Agent-Prozedur • 10
Richtlinien – Registerkarte "Einstellungen" – Alarme unterbrechen • 28
Richtlinien – Registerkarte "Einstellungen" – Anmeldedaten • 14
Richtlinien – Registerkarte "Einstellungen" – Anmeldung • 12
Richtlinien – Registerkarte "Einstellungen" – Arbeitsverzeichnis • 30
Richtlinien – Registerkarte "Einstellungen" – Auditplan • 12
Richtlinien – Registerkarte "Einstellungen" – Automatische Windows-Aktualisierung patchen • 24
Richtlinien – Registerkarte "Einstellungen" – Benachrichtigungen • 10
Richtlinien – Registerkarte "Einstellungen" – Datei verteilen • 15
Richtlinien – Registerkarte "Einstellungen" – Ereignisprotokolleinstellungen • 15
Richtlinien – Registerkarte "Einstellungen" – Kaseya AntiMalware • 16
Richtlinien – Registerkarte "Einstellungen" – Kaseya Antivirus • 16
Richtlinien – Registerkarte "Einstellungen" – Kaseya Security • 16
Richtlinien – Registerkarte "Einstellungen" – LAN-Cache • 17
Richtlinien – Registerkarte "Einstellungen" – Liste nach Scan aktualisieren • 29
Richtlinien – Registerkarte "Einstellungen" – Monitor-Sets • 18
Richtlinien – Registerkarte "Einstellungen" – Neustart für Softwarebereitstellung • 26
Richtlinien – Registerkarte "Einstellungen" – Patchdateiquelle • 19
Richtlinien – Registerkarte "Einstellungen" – Patch-Einstellungen • 23
Richtlinien – Registerkarte "Einstellungen" – Patch-Neustart-Aktion • 21
Richtlinien – Registerkarte "Einstellungen" – Patch-Verfahren-Planung • 20
Richtlinien – Registerkarte "Einstellungen" – Protokollhistorie • 17
Richtlinien – Registerkarte "Einstellungen" – Rechnerprofil • 18
Richtlinien – Registerkarte "Einstellungen" – Remote Control • 25
Richtlinien – Registerkarte "Einstellungen" – Schutz • 24
Richtlinien – Registerkarte "Einstellungen – Zuweisung Softwarebereitstellungsprofil • 26
Richtlinien – Registerkarte "Einstellungen" – Zuweisung Softwarebereitstellungsscan • 28
Richtlinien und Ansichten • 39
Richtlinienmatrix • 4
Richtlinienstatussymbol • 40
Richtlinienüberschreibungen • 40

S

SaaS • 40
Software as a Service (SaaS) • 40
System-Cabinets • 40

T

Tenant-Partition • 40
Token • 41